

A TRUE COPY

May 15, 2023

s/ D. Olszewski

Deputy Clerk, U.S. District Court
Eastern District of Wisconsin

UNITED STATES DISTRICT COURT

for the
Eastern District of WisconsinIn the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)Records and information associated with 17
social media accounts (See Attachments)Case No. 23 MJ 91
Matter No.: 2022R00210

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See Attachment A. Over which this Court has jurisdiction pursuant to 18 U.S.C. §§ 2703 and 2711 and Federal Rule of Criminal Procedure 41.

located in the _____ District of _____, there is now concealed (identify the person or describe the property to be seized):

See Attachment B.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

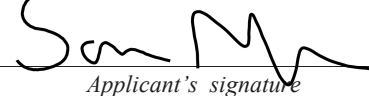
The search is related to a violation of:

Code Section	Offense Description
18 U.S.C. § 371; 18 U.S.C. § 1343; 21 U.S.C. § 841; 26 U.S.C. § 7206	Conspiracy to violate the laws of the United States; wire fraud; unlawful possession and distribution of controlled substances; false statement in connection with tax submission

The application is based on these facts:

See the attached affidavit.

- ☒ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.



Applicant's signature

SA Sarah Mazur, FBI

Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by
_____ telephone _____ (specify reliable electronic means).

Date: 5/15/2023



Judge's signature

City and state: Milwaukee, WI

Hon. William E. Duffin, U.S. Magistrate Judge

Printed name and title

**AFFIDAVIT IN SUPPORT OF AN
APPLICATION FOR A SEARCH WARRANT**

Matter No. 2022R00210

I, FBI SA Sarah Mazur, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information associated with the accounts listed below. Information pertaining to these accounts is stored at premises owned, maintained, controlled, or operated by Meta Platforms (“Meta”), a social networking company headquartered at 1601 Willow Road, Menlo Park, California, 94025, further described herein and in Attachment A respectively (attached hereto and incorporated herein:

- a. Facebook Account: UID: 103183581120331 (**Target Account 1**)
- b. Facebook Account: UID: 100004443158401 (**Target Account 2**)
- c. Facebook Account: UID: 100063503829690 (**Target Account 3**)
- d. Facebook Account: UID: 1003158861 (**Target Account 4**)
- e. Facebook.com/bighomie.rob; UID: 100037412529073 (**Target Account 5**)
- f. Instagram.com/millionairementality; UID: 210030646 (**Target Account 6**)
- g. Facebook Account: UID: 100013113481774 (**Target Account 7**)
- h. Facebook Account: UID: 100063752476178 (**Target Account 8**)
- i. Instagram Account: UID: 1296285044 (**Target Account 9**)
- j. Facebook Account(Group): 229347966182445. URL:
facebook.com/groups/229347966182445 (**Target Account 10**)
- k. Facebook Account(Group): 545401084294236. URL:
facebook.com/groups/545401084294236 (**Target Account 11**)
- l. Facebook Account;; UID: 100033707269327 (**Target Account 12**)

- m. Instagram.com/mr_david_martin UID: 341470073 (**Target Account 13**)
- n. Facebook Account: UID: 100063561696774 (**Target Account 14**)
- o. Facebook Account: UID: 100063862190767 (**Target Account 15**)
- p. Instagram Account: UID: 26331965215 (**Target Account 16**)
- q. Facebook Account (Group) UID 242867438180983, URL:
<https://www.facebook.com/groups/242867438180983> (**Target Account 17**)

2. I have been a Special Agent with the Federal Bureau of Investigation (“FBI”) for eight years. I am currently assigned to the Milwaukee Division’s Joint Terrorism Task Force, where I investigate and assist in matters involving violations of federal law related to international terrorism, domestic terrorism, and sovereign citizen financial crimes. Prior to my time in Milwaukee, I spent approximately five years as a Special Agent in Boston investigating violent street gangs. My training and experience include the execution of arrest warrants and search warrants, including search warrants involving electronic evidence.

3. I am an investigative or law enforcement officer of the United States within the meaning of Title 18, United States Code, Section 2510(7), in that I am empowered by law to conduct investigations of and to make arrests for federal offenses.

4. The facts in this affidavit come from my personal observations, my training and experience, my review of documents, and information from other law enforcement officers and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

5. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other law enforcement officers and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

6. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that (i) violations of 18 U.S.C. § 371 (conspiracy to violate the laws of the United States); 18 U.S.C. § 1343 (wire fraud); 21 U.S.C. § 841 (unlawful possession and distribution of controlled substances); and 26 U.S.C. § 7206 (false statement in connection with tax submission) (the “Subject Offenses”) have been committed by Caliph MUAB-EL (“MUAB-EL”) aka Anthony Stevens, Ladrea LAMON (“LAMON”), Jessica MARTIN (“MARTIN”), and David Martin (“DAVID”) and (ii) evidence probative of the same will be found in the data sought by the instant warrant. There is therefore probable cause to search the information described in Attachment A for evidence of these crimes further described in Attachment B.

PROBABLE CAUSE

BACKGROUND ON THE NATION OF MOORS AND BLACK P STONE NATION (BPSN)

7. In May 2022 the Milwaukee Division of the FBI opened an investigation pertaining to CALIPH MUAB-EL (“MUAB-EL”), whom law enforcement believes is a high-ranking member of the Black P Stone Nation (“BPSN”). The BPSN is a highly structured and organized violent gang operating in various jurisdictions, including the Eastern District of Wisconsin.

8. The BPSN has written recruiting procedures and upon joining, new members must recite loyalty pledges verbatim. In addition, the BPSN “ranks” its male and female members according to their seniority in the organization. On or about November 14, 2022, a confidential human source (hereinafter referred to as CHS1) provided law enforcement with a document entitled “The Proper People Procedures from the Chief Mustafa Malik Ang-El”. This document appeared to outline the history, leadership structure, and hierarchy of the BPSN. The document explained the organization had the following membership hierarchy, ranked from highest to lowest:

- a. Chief - Mustafa Malik Ang-El
- b. Crown Prince – Mustafa Mustafa
- c. Grand Sheik/Prince
 - i. Investigation thus far led law enforcement to believe that MUAB-EL holds the position of Grand Sheik or Prince within the BPSN.
- d. Assistant Grand Sheik/Akbar
- e. Chairman/General
- f. African Shield
- g. Mufti Ranger
- h. Soldier

CHS DISCLOSURES

CHS#1

9. The majority of CHS #1's information has been corroborated by law enforcement. CHS #1 has an extensive criminal history and multiple felony convictions, including violations of probation and robbery with the use of force. CHS #1 worked for law enforcement and was paid as a source for approximately three months before being arrested in 2022 on charges regarding firearms and narcotics. Despite the recent arrest, case agents believe that the successful corroboration of the majority of CHS #1's reporting suggests the information previously provided and recounted here was reliable.

CHS #2

10. The majority of CHS #2's information has been corroborated by law enforcement or has been recorded. CHS #2 has an extensive criminal history and felony convictions, including violations of laws prohibiting the intimidation of victims and the use of force. CHS#2 began

working for law enforcement in March 2023 for consideration on a state criminal charge. CHS#2 has also been compensated for his cooperation by law enforcement.

BACKGROUND PPP/EIDL LOANS

11. The United States Small Business Administration (“SBA”) is an executive branch agency of the United States government that provides support to entrepreneurs and small businesses. As part of this effort, the SBA enables and provides for loans through banks, credit unions, and other lenders.

12. The Coronavirus Aid, Relief, and Economic Security (“CARES”) Act was a federal law enacted in or around March 2020 and designed to provide emergency financial assistance to the millions of Americans suffering the economic effects caused by the COVID-19 pandemic. One source of relief that the CARES Act provided was the authorization of forgivable loans to small businesses for payroll, mortgage interest, rent/lease, and utilities, through the Paycheck Protection Program (“PPP”).

13. To obtain a PPP loan, a qualifying business was required to submit a PPP loan application, which was signed by an authorized representative of the business. The PPP loan application required the business (through its authorized representative) to acknowledge the program rules and make certain affirmative certifications in order to be eligible to obtain the PPP loan. In the PPP loan application, the small business (through its authorized representative) had to state, among other things, its average monthly payroll expenses and number of employees. These figures were used to calculate the amount of money the small business was eligible to receive under the PPP.

14. Businesses were required to use PPP loan proceeds on payroll costs, interest on mortgages, rent, and utilities. The PPP allowed the interest and principal on the PPP loan to be

entirely forgiven if the business spent the loan proceeds on these expense items within a designated period of time and used a certain percentage of the PPP loan proceeds on payroll expenses.

15. The SBA oversaw the PPP. However, individual PPP loans were issued by private, approved lenders who received and processed PPP applications and supporting documentation, and then made loans using the lenders' own funds, which were 100 percent guaranteed by the SBA.

16. The CARES Act also expanded the separate Economic Injury Disaster Loan ("EIDL") Program, which provided small businesses with low-interest loans up to \$2 million prior to in or about May 2020 and up to \$150,000 beginning in or about May 2020, which can provide vital economic support to help overcome the temporary loss of revenue they are experiencing due to COVID-19. To qualify for an EIDL loan under the CARES Act, the applicant must have suffered "substantial economic injury" from COVID-19, based on a company's actual economic injury determined by the SBA, up to \$2 million. EIDLs may be used for payroll and other costs as well as to cover increased costs due to supply chain interruption, to pay obligations that cannot be met due to revenue loss, and for other similar uses. The CARES Act also permitted applicants to request an advance of up to \$10,000 to pay allowable working capital needs, which was expected to be paid by the SBA within three days of submission of an EIDL application to the SBA, provided the application contains a self-certification under penalty of perjury of the applicant's eligibility for an EIDL. Unlike the PPP, the SBA directly makes loans to applicants under the EIDL Program.

NON-PROFIT ORGANIZATIONS CONNECTED TO MUAB-EL
BREAKING BARRIERS BREAKING BARRIERS MENTORING (WISCONSIN)

17. MUAB-EL was previously sentenced to 15 years in prison for reckless injury with use of a dangerous weapon and released in 2012. Since 2012, MUAB-EL has sought out inmates at correctional facilities, ostensibly to assist their transition back into society. MUAB-EL seeks

out donations and grants to obtain funding to be used in mentoring and community outreach and activism. According to the Wisconsin Department of Financial Institutions (“DFI”), MUAB-EL is listed as the registered agent of Breaking Barriers Mentoring (Wisconsin) Inc. (“BBM”). The website for BBM describes BBM as a local nonprofit based in Milwaukee serving individuals who have been incarcerated.

18. On or about April 2, 2020, MUAB-EL applied for an EIDL loan for BBM. On the application MUAB-EL stated BBM had three employees. According to payroll records reviewed by law enforcement, BBM only pays one employee, which is MUAB-EL. BBM received an approximate total of \$56,900 of EIDL money, of which the majority was paid to MUAB-EL in the form of payroll.

19. BBM’s reported mission is to educate, support and uplift individuals who have been incarcerated. However, approximately 78% of the expenses from BBM is paid to MUAB-EL through payroll expense or money transfers.

ALL OF US OR NONE WISCONSIN

20. Per DFI, MUAB-EL is also the registered agent for All of Us Or None Wisconsin, LLC (“AOUON”). According to the AOUON website, MUAB-EL is listed as the President of its Wisconsin chapter. The website also provides a biography of MUAB-EL and describes his ostensible commitment to helping the community.

21. MUAB-EL confided in CHS1 that AOUON was a front used to get free money from the government. MUAB-EL learned, from other Moors and BPSN members, how to develop and manage non-profit organizations for the purposes of committing fraud. MUAB-EL instructed CHS1 to attend an AOUON meeting, so he could put his/her information into a computer system where it would list CHS1 as an employee even though he/she was not actually working for the

company. After becoming an employee, CHS1 would receive a paycheck twice a month and would need to give a portion of the money to MUAB-EL. MUAB-EL also stated MUAB-EL would receive \$2,000 in life insurance money for the CHS1 and would provide some of the money to the CHS1. MUAB-EL stated AOUON has about 500 employees. According to information received from the Wisconsin Department of Workforce Development (“DWD”), AOUON has not filed any wage reports with the state of Wisconsin.

22. MUAB-EL applied to receive two EIDL loans for AOUON. The loans were not approved. On one application MUAB-EL represented AOUON was established on or about June 10, 2020, while another application MUAB-EL represented AOUON was established on or about February 1, 2017. The first application, dated on or about July 8, 2020, stated AOUON had one employee, but the second application, dated on or about March 31, 2021, stated AOUON had seven employees. Records reviewed for AOUON showed AOUON does not have payroll expenses. The majority of revenue coming in to AOUON is spent on Cash App transactions as opposed to business related expenses.

23. CHS #1 provided the BPSN is closely connected to the Moorish Science Temple of America (“MSTA”). MUAB-EL is also the Grand Sheik of the MSTA located in the Milwaukee area. CHS #1 reported MSTA was also associated with AOUON, which MUAB-EL uses to commit various crimes and fraud.

PPP LOANS

24. MUAB-EL was featured in an article on the Juvenile Justice Information Exchange about not being able to obtain Paycheck Protection Program money for BBM due to his criminal history. However, legal process revealed that MUAB-EL applied for and received two PPP loans

for a sole proprietorship in his name. Searches on DFI and law enforcement databases yielded no results for a company called Caliph Muab-El.

25. Legal process revealed that MUAB-EL applied for a PPP loan that was approved by Cross Riverbank on or about April 2, 2021. Cross Riverbank provided the loan was funded on or about April 5, 2021. MUAB-EL purported the company was established in 2017, he was the only employee, and the business had 2020 net profit of \$104,133. MUAB-EL provided a photo of his driver's license when applying for the loan.

26. On or about April 6, 2021, MUAB-EL received \$20,833 in his personal bank account held with Summit Credit Union. Records revealed that the same day he received these funds, he transferred \$10,000 to his savings account but transferred \$5,000 back to his checking account on or about April 8, 2021. On or about April 7, 2021, records indicate MUAB-EL sent approximately \$5,000 to "Brianna L." Law enforcement believes Brianna L to be Brianna Nelson, because (i) an individual with that name is connected to AOUON per the AOUON website; and (ii) other legal process revealed that MUAB-EL sent cash app payments to Brianna L Nelson. On or about April 8, 2021, MUAB-EL took out a vehicle loan with Summit Credit Union for a 2017 Lincoln. MUAB-EL provided a \$6,000 down payment with the vehicle.

27. On or about April 22, 2021, MUAB-EL was approved for a second draw of PPP loan through Prestomas CDFI, LLC ("Prestomas"). Prestomas provided that the loan of \$20,832 was disbursed on or about April 28, 2021. The loan documents associated with this loan provided that MUAB-EL's sole proprietorship was established in 2020. MUAB-EL provided a copy of 2020 Schedule C (Form 1040) Profit or Loss from Business with his loan application; however, this Schedule C (Form 1040) was not filed with the IRS.

28. On or about May 7, 2021, MUAB-EL received \$20,832 for this additional PPP loan into his personal checking account. On or about the same day, MUAB-EL made a \$1,000 loan payment, transferred \$5,000 to his savings, and withdrew \$3,000 in cash. On or about May 10, 2021, MUAB-EL made a credit card payment of approximately \$2,000.

29. Both loan agreements associated with the PPP loans discussed above include the following question: “Is the Applicant or any owner of the Applicant an owner of any other business, or have common management (including a management agreement) with any other business? If yes, list all such businesses (including their TINs if available) and describe the relationship on a separate sheet identified as addendum A.” MUAB-EL answered “no” to the question both times. A record check on the DFI website shows that MUAB-EL is the registered agent of five businesses including BBM and AOUON. MUAB-EL provided bank statements for February 2020 and February 2021 as supporting documentation for the loan. The bank statement provided for February 2020 provided MUAB-EL received \$833 from BBM. The February 2021 bank statement provided MUAB-EL received a total of \$1,750 from AOUON in his checking and savings accounts and a \$3,000 deposit from BBM. Subpoenaed payroll records from BBM revealed that MUAB-EL received wages of approximately \$73,550 in 2020 and approximately \$72,500 in 2021.

Narcotics Trafficking

30. On or about November 14, 2022, law enforcement met with CHS #1 in order to conduct a controlled substance purchase from MUAB-EL. Earlier in the day, CHS1 contacted MUAB-EL and stated that CHS #1 was going to MUAB-EL’s residence. A Pen Register Trap and Trace on the **MUAB-EL** cell phone corroborated CHS1’s contact with MUAB-EL.

31. CHS #1 was provided buy money and searched for contraband, finding none. CHS #1 was monitored constantly by surveillance squads after being searched. As more fully detailed

below, CHS #1 provided MUAB-EL with the buy money in exchange for heroin. CHS #1 then met with law enforcement and gave law enforcement an amount of heroin. CHS1 was again searched for money or contraband, finding none.

32. The operation took place in two locations, one for the payment and another for the transfer of narcotics. At the first location, CHS1 provided \$10,000 to MUAB-EL, who ran it through money counter with another individual, to ensure it was the correct amount. Further, MUAB-EL made CHS1 aware that \$7,000 of the payment would be brought to “Rafael” and the remaining \$3,000 would be kept for the “nation” (the term “nation” is believed by law enforcement to refer to the gang as a whole). This information is consistent with what the affiant heard over the transmitter in real-time.

33. On the way to the second location, MUAB-EL picked up “Chairman Tezz” (known by law enforcement to be Franklin D. Maurtz, DOB 07/27/1985, hereinafter MAURTZ). CHS1 stated MAURTZ had approximately 30 grams of heroin, approximately a pound of marijuana, and an Uzi-style firearm when MUAB-EL picked him up. CHS1 later advised case agents that MAURTZ oversaw security for MUAB-EL and cooked (a term used to describe the process of converting cocaine powder into cocaine base) narcotics for MUAB-EL. After arriving at the second location, 5315 North Milwaukee River Parkway, Milwaukee, Wisconsin, MUAB-EL retrieved the suspected heroin from the freezer in the kitchen and pulled out three “50’s” (packages containing 50 grams of heroin), which were wrapped in black duct tape. MAURTZ then assisted MUAB-EL by cutting and weighing the narcotics before presenting them to CHS1. Based on my training and experience, I am aware that narcotics traffickers often keep specific aspects of the illicit business separate from each other. For example, narcotics will often be stored in one house

and money in another. Spreading assets limits the loss to the trafficker in the event of theft or law enforcement action.

34. At the conclusion of the purchase, CHS1 provided the narcotics to law enforcement who also search both CHS1 and CHS1's vehicle for contraband, though none was found. The heroin purchased during the controlled evidence purchase mentioned above was field tested by law enforcement and did test positive for the probable presence of Heroin/Opiates – Possible Fentanyl.

35. CHS1 also reported that he had observed MUAB-EL weighing suspected narcotics in approximately October 2022. CHS1 reported that MUAB-EL transported some of the drugs to Madison and some to Milwaukee. MUAB-EL informed CHS1 that "Cubans" in Kenosha were a major source of his supply for heroin and cocaine.

36. CHS1 later identified the source of supply in Kenosha as Mustafa Ra'El (ANDERSON) (known to law enforcement to be Miles Anderson). CHS1 provided the phone number for ANDERSON and positively identified him from photos. CHS1 has been inside ANDERSON's home in Kenosha, WI and has seen illegal drugs inside the residence. Records reviewed associated with MUAB-EL's cell phone revealed ANDERSON was a top contact of MUAB-EL. Between October 25, 2022, and November 21, 2022, MUAB-EL had approximately 34 calls and 129 texts with ANDERSON.

37. Records reviewed associated with MUAB-EL's cell phone revealed that Jerry MCCOY is another top contact for MUAB-EL. CHS #1 reported that MCCOY is MUAB-EL's source of supply for Marijuana. CHS #1 reported MCCOY also is MUAB-EL's partner for a hemp store located in Milwaukee, WI.

BPSN VIOLENCE

38. On or about November 8, 2022, CHS1 reported to law enforcement regarding an incident that took place involving MUAB-EL and “Rich” (known by law enforcement to be Troy Randle Jr, DOB 07/27/1996, hereinafter RANDLE). RANDLE called CHS1 in the middle of the night on or about November 6, 2022, to tell CHS1 that he had been placed “under arrest” by members of the BPSN and the leader of the Gangster Disciples gang in Milwaukee, known to CHS #1 as “Reese”. CHS1 explained that MUAB-EL kicked RANDLE out of the BPSN for breaking several of the group’s laws. For example, MUAB-EL believed RANDLE stole 150 grams of heroin from the group. RANDLE also had firearms belonging to MUAB-EL. RANDLE was eventually let go with the understanding that RANDLE would meet with MUAB-EL the next day. However, when RANDLE failed to show, MUAB-EL and a number of BPSN members travelled to RANDLE’s mother’s house and “arrested” her boyfriend, threatening to remove a limb for every hour that RANDLE was late. MUAB-EL instructed BPSN members present to put RANDLE’s mother’s boyfriend in the back of an SUV. More BPSN members arrived until the group number was approximately 30 people, but RANDLE still failed to come. While waiting for RANDLE to arrive, shots were fired at the group from an unknown location. Approximately 12 of those shots struck the SUV where RANDLE’s mother’s boyfriend was being kept. CHS #1 indicated that after the shots were fired, the BPSN members left, and MUBA-EL allowed RANDLE’s mother’s boyfriend to leave due to the fact the police were responding to the scene.

39. According to CHS1, MUAB-EL believed that RANDLE was responsible for the shooting, and further believed that he was a liability due to his knowledge about the group. For these reasons, MUAB-EL spoke to multiple individuals about killing RANDLE. CHS #1 explained that MUAB-EL would likely pay them in heroin or lower the price per gram MUAB-EL was currently charging them if they killed RANDLE.

40. On or about November 6, 2022, District Seven of the Milwaukee Police Department (MPD) dispatched officers to 3718 North 92nd Street, Milwaukee, Wisconsin, where a threat had turned into a shots fired incident following a tip from an anonymous caller (MPD Incident No. 223100138). The caller stated that she and her son were receiving calls and texts from a subject identified as “Caliph MuabEl”. The caller stated that the subject had been making threats to kill her and her family and calling and/or texting constantly in an attempt to locate her son. An officer dispatched to the scene located seven shell casings from a 9mm and 380 firearms.

41. On or about November 15, 2022, CHS #1 provided he/she was contacted by MUAB-EL via cell phone. CHS #1 received a text that stated “Emergency. My uncle the P just passed.” Based on prior information CHS #1 received, CHS #1 believed MUAB-EL was going to order someone in Chicago to get killed at the direction of MUAB-EL for retaliation of his uncle’s death.

42. On or about October 29, 2022, CHS #1 consensually recorded a conversation with MUAB-EL about MUAB-EL taking a trip to Florida to beat up an Assistant Grand Sheikh or AGS who lived in Florida. MUAB-EL stated the AGS was not following the BPSN/Moor law and needed to be punished. On a separate occasion, MUAB-EL confided in CHS #1 that MUAB-EL drove to Florida with others to punish the AGS. MUAB-EL stated they broke the AGS’s feet, hands, and cut his tongue down the middle. MUAB-EL said the AGS was going to look like a snake because he was a snake. CHS #1 learned the BPSN have a Facebook page that displays much of the violence carried out by the gang. Only certain members of the gang have access to the site. A member of the group posted a Facebook video of AGS, who was breathing heavily and appeared to be distraught. The purpose of the video was for the AGS to apologize for his violations of gang protocol. CHS #1 provided a copy of this video to law enforcement.

43. On or about October 29, 2022, CHS #1 consensually recorded a conversation with MUAB-EL where he stated he needed a new butterfly knife. MUAB-EL stated he cut someone with it and messed them up with it and threw that knife in the sewer. The knife he used was MUAB-EL's favorite. MUAB-EL stated that cutting someone's throat was clean and you did not have to worry about getting caught.

44. On or about March 13, 2023, CHS #2 made a recorded call with MUAB-EL. During that call, MUAB-EL represented that he wanted CHS #2 to go down to Chicago for a meeting with "some very important people". MUAB-EL stated they were people in CHS #2's "division". Law enforcement believes this to be a reference to members of the gang CHS #2 belongs to. MUAB-EL then listed off various gangs to CHS #2 and stated he was the "Divine-Minster" over the various gangs.

THE FAMILY FIRST CORONAVIRUS RESPONSE ACT (FFCRA)

45. The Family First Coronavirus Response Act (FFCRA), passed in March 2020, allowing eligible self-employed individuals who, due to COVID-19 are unable to work or telework for reasons relating to their own health or to care for a family member to claim refundable tax credits to offset their federal income tax. The credits are equal to either their qualified sick leave or family leave equivalent amount, depending on circumstances.

46. Eligible self-employed individuals must conduct a trade or business that qualifies as self-employment income and be eligible to receive qualified sick or family leave wages under the Emergency Paid Sick Leave Act or Emergency Family and Medical Leave Expansion Act as if the taxpayer was an employee.

47. The credits can be claimed on multiple individual and business tax forms. For individual tax returns they are claimed on Form 7202, Credits for Sick Leave and Family Leave

for Certain Self-Employed Individuals or Schedule H Household Employment Taxes. These credits flow through the Schedule 3 Additional Credits and Payments and finally to the Form 1040 U.S. Individual Tax Return.

48. Taxpayers claim the tax credits for leave taken between April 1, 2020, and December 31, 2020, on their tax year 2020 return. Taxpayers claim the credit for leave taken between January 1, 2021, and September 30, 2021, on their tax year 2021 return. The total credit is separated between leave taken through March 31, 2021, and leave taken April 1, 2021, and after. This is due to the extension of the credit by the Tax Relief Act.

TAX SCHEME

49. On multiple occasions MUAB-EL discussed MUAB-EL's involvement in a tax fraud scheme with CHS #1. MUAB-EL told CHS #1 that he is a partner with Empire Tax Firm, which prepares tax returns with fraudulent information for the purposes of getting a tax refund of over \$20,000. MUAB-EL receives a portion of the funds for every person who submits a false tax return.

50. On or about October 29, 2022, CHS #1 consensually recorded MUAB-EL talking about the tax scheme and stating that he (MUAB-EL) was going to get a lot of money from it. Another individual present for the recording stated everyone in his house was going to submit the returns by the end of November 2022. MUAB-EL stated he had a list of twenty-five people who would be the first to complete the tax fraud. On or about November 9, 2022, CHS #1 consensually recorded MUAB-EL again talking about the tax scheme. MUAB-EL stated people could get a lot of money from the IRS for individuals claiming to be sole proprietors. MUAB-EL stated a personal move could be paid by the IRS if you set it up with tax credits. He further claimed that once Empire Tax firm calculates the refund the person can also take out a separate cash advance. MUAB-EL said "the Agency charges 10" but the person will get no less than \$15,000 to \$20,000

per person. MUAB-EL stated it was simple for everyone to get their “bread,” which law enforcement knows is common vernacular for money. MUAB-EL stated someone can do this once a year. MUAB-EL stated that in 2023, the amount will go up because of different tax credits. MUAB-EL stated participating in this scheme will also boost their credit scores.

51. CHS#1 was informed someone would need the following information to participate in the scheme:

- a. Picture of Identification
- b. Social Security Number
- c. Email address
- d. Mailing address
- e. Phone number
- f. Bank Account and Routing number

52. MUAB-EL informed CHS#1 if someone did not have a bank account, they could still participate in the scheme using prepaid cards.

53. CHS #1 informed MUAB-EL that he/she had no W2's or income to report on a tax return. MUAB-EL indicated this would not be an issue, and that the person at Empire Tax Firm will create all the necessary paperwork.

54. MUAB-EL provided CHS #1 the contact number for the person helping MUAB-EL with the tax scheme as 414-949-0684. Legal process revealed that this number was subscribed to by Ladrea LAMON. MUAB-EL informed CHS #1 that for CHS #1 to participate in the scheme, CHS #1 needed to send his/her information to that number. Phone records reviewed associated with MUAB-EL's number, between October 25, 2022, and November 21, 2022, revealed MUAB-EL had approximately 23 phone calls and 131 texts with LAMON.

55. CHS#1 provided that the email address moorsunite87@gmail.com is the email address used to facilitate this fraud involving MUAB-EL. On or about October 30, 2022, that same email address sent a copy of a false return to CHS #1, which CHS #1 provided to law enforcement. The return was a 1040 Individual Tax Return for year 2021. The return listed CHS #1 as a self-employed contractor/painter. CHS #1 confirmed none of the information in the return was true. The return also included a Schedule C (Profit and Loss statement) for the fabricated “business.” The return also had CHS #1’s banking information which he/she stated he/she did not provide because that account was closed. Law enforcement suspects that the individual who prepared the fraudulent return received this information from a prior tax return. The refund that CHS #1 would receive, per the false return, was to be \$21,800, and CHS #1 understood they were expected to pay MUAB-EL and LAMON a portion of that money.

56. On or about March 22, 2023, CHS #2 made a consensually recorded call with MUAB-EL about the tax scheme. MUAB-EL said he already got his tax money this year. MUAB-EL stated he would reach out the next day to CHS #2 and get him introduced to the “Sister”. MUAB-EL stated he thinks CHS #2 will get a refund around \$35,000, but at least \$20,000. MUAB-EL told CHS #2 the tax preparer will take out fees. MUAB-EL stated CHS #2 could do that for anyone that is over age of 18. MUAB-EL said the process takes about two and a half weeks, and if CHS #2 has five trustworthy people, CHS #2 can do the tax thing as well and take a cut of those tax refunds. MUAB-EL told CHS #2 they need copy of ID and social security card.

57. On or about April 4, 2023, CHS #2 made a consensually recorded call with LAMON at number 414-949-0684 about the tax scheme. LAMON told CHS #2 about the forms of ID that were needed. LAMON said every tax return is different, but she will let CHS #2 know what the amount is. LAMON stated her fee comes off the top, but CHS #2 would need to meet

with MUAB-EL to give him his cut. LAMON said she works for a firm and the firm charges a percentage, but CHS #2 would pay MUAB-EL a fee and MUAB-EL would pay Lamon the other part of her fee since she does not know CHS #2. LAMON stated she is getting people back the max refund and fixing their credit. LAMON stated she is still waiting on her tax refund and her boss filed her tax return. LAMON talked about doing MUAB-EL's tax return this year with CHS #2.

58. LAMON is listed as the preparer of MUAB-EL's filed 2022 tax return. The refund claimed on MUAB-EL 2022 tax return is \$12,930. MUAB-EL's tax return included a Schedule C, Profit or Loss from Business, for a petroleum business, which is a different type of business than listed on his 2020 Schedule C used to apply for a PPP loan. MUAB-EL and LAMON have approximately 12 calls and 15 texts between March 6 and March 23, 2023.

59. LAMON advertises about preparing taxes on her Facebook page. The phone number and Tax Firm listed on LAMON's Facebook posts corroborates information provided by CHS#1.

60. A citizen witness ("KC"), who was a former tax preparer for Empire Tax firm, provided that the owner of Empire Tax Firm, Jessica Martin (MARTIN), needed to review all tax returns before they were submitted. KC stated that she used her personal email address when preparing tax returns because MARTIN required employees to purchase a company email account from her. KC emailed info@etaxfirms.com when she needed a return reviewed. KC stated that trainings related to EMPIRE took place over Zoom and through Facebook groups.

61. CHS #1 provided that MUAB-EL uses Cash App to send and receive money relating to fraud.

62. On or about April 12, 2023, CHS #2 reached out to LAMON via text. Lamon responded that CHS#2's taxes were in review and was waiting on numbers. Based upon other information received, the affiant believes that this means the return was submitted to MARTIN for fraudulent credits and information to be inputted in the return.

EMPIRE TAX FIRM

63. MARTIN and DAVID are the listed owners of EMPIRE. Beginning in February 2023 the FBI and IRS started receiving tips from citizens that EMPIRE and MARTIN were preparing fraudulent tax returns.

64. A Citizen Witness ("LW") stated LW grew up with MARTIN in Rockford, IL. LW reached out to MARTIN for an estimate to have LW's taxes completed. MARTIN sent LW a link for LW to fill out some personal information. LW filled out the information and received notification that her refund would be \$13,946 and EMPIRE would take fees of approximately \$2,300. LW told the FBI she was confused because she reached out for an estimate and thought the refund amount was high. LW stated she did not give MARTIN or EMPIRE permission to file her taxes, especially since LW did not review the return prior to filing. LW reached out to the IRS who confirmed a return was filed by EMPIRE and LW received her transcripts from the IRS. LW stated the return provided by the IRS created by EMPIRE was fraudulent. The return included a profit and loss statement for a company in LW's name. LW told the FBI that LW does not have a business and the return had fraudulent amounts in it.

65. After learning of the fraudulent return, LW posted about MARTIN and EMPIRE on her Facebook page. The post caused a negative reaction from MARTIN. LW reported that MARTIN made Facebook live videos about LW and others who said EMPIRE was committing fraud. LW stated MARTIN was from a dangerous family and thought MARTIN was connected

to a gang, the “Moes”. Law enforcement believes the term “Moes” could be another term for BPSN.

66. Another citizen witness (“SS”) reported to the FBI that MARTIN and EMPIRE filed fraudulent taxes for SS. SS provided her return was filed without her permission or review. When SS asked questions about her return, an EMPIRE employee sent it to her. SS provided that this employee was now fired. SS stated that MARTIN told tax clients she would not let anyone see their return until after April 15th. SS provided her tax return prepared by EMPIRE to law enforcement and stated the amounts on the return were fraudulent. The preparer on the return was Jonathon Ellis, MARTIN’s brother. The return provided to SS by EMPIRE was missing Schedule 3. Schedule 3 was used to claim a tax credit SS did not qualify for, causing a higher tax refund to be claimed for SS.

67. SS stated that MARTIN was creating Facebook live videos about SS that SS viewed as threatening. SS provided law enforcement screenshots and copies of Facebook live videos she recorded of MARTIN. In the videos MARTIN talks about amending tax returns and that EMPIRE employees did make mistakes by not having clients sign to approve the return.

68. Another citizen witness (“MP”) contacted the FBI about MARTIN and EMPIRE. MP was a tax preparer working under MARTIN. MP stated MARTIN is from Rockford, IL and she became aware of MARTIN’s credit repair business, EMPIRE YOU, LLC, and her tax business, EMPIRE, through social media.

69. To earn extra money MP decided to prepare taxes for EMPIRE and paid for the training classes offered by MARTIN. MP estimated she completed approximately 8 to 10 trainings, and she did not feel she knew enough to prepare taxes after the trainings. MP stated the trainings went over basic procedures on how to input clients’ information into the tax software; no in-depth

training on tax preparation was given. As part of the training, MP got a Preparer Tax Identification Number (PTIN) use when preparing taxes. MP estimated she entered information into the EMPIRE's tax software for approximately eighteen clients.

70. MP stated she did not have a company email and used her personal email to communicate with MARTIN and EMPIRE. Another citizen witness ("KC") stated she also used a personal email address when communicating with MARTIN because she did want to pay to receive a company email.

71. After MP entered in client information into the EMPIRE's tax software, MP marked the file as needing review. During that stage, EMPIRE's review team reviewed the file and filed the tax return with the IRS. MP initially believed EMPIRE's review team was people who worked for MARTIN but now MP suspects MARTIN was the only one reviewing the tax returns. MP did not see the returns before they were filed and did not personally file any of the taxes with the IRS. MP realized that fraud was being committed when one of her clients was contacted by the IRS to verify information. Upon review of that tax return, MP realized the return claimed a fraudulent daycare business that MP did not enter into the tax software.

72. MP also filed her own tax returns with EMPIRE. MP stated MARTIN prepared her 2021 and 2022 tax returns. MP did not review the returns before they were filed. MP stated she does not have a beauty salon business making her past two tax returns filed by MARTIN fraudulent. MP only dealt with MARTIN to prepare her tax returns; however, another preparer is listed as the return preparer on MP's 2022 tax return. MP does not know the preparer listed.

73. LW continues to provide information she learns about EMPIRE. LW provided she created a group where victims of EMPIRE can communicate about the fraud and help each other file amended returns. As part of this group, LW learned MARTIN was possibly using tax client

social security numbers to take out lines of credit or loans without clients' knowledge. It is possible EMPIRE is doing this in conjunction with their credit repair business, EMPIRE YOU LLC.

74. LW also provided Facebook and Instagram Live videos of MARTIN discussing the tax business and other businesses. During the video MARTIN discussed that at most clients would get for filing returns with fraudulent credits is a \$500 fine. In addition, in one of the videos MARTIN stated the purpose of being a tax preparer is to get clients to qualify for tax credits they do not qualify for.

TARGET ACCOUNT 1

75. **Target Account 1** is associated with AOUON. According to records received from Facebook, the creator of the account is MUAB-EL. The page has private messages enabled. Figures 1 and 2 below are screenshots taken from **Target Account 1** on or about March 8, 2023. The first screenshot (Figure 1) is what the account looks like when clicking on the page. The second screenshot (Figure 2, depicting MUAB-EL) was posted on or about September 6, 2022. Given the evidence discussed above vis-à-vis AOUON, MUAB-EL's connection to **Target Account 1**, the targets' use of social media to advance their misconduct, and the private messages associated with **Target Account 1**, I believe this account is likely to contain communications or information pertaining to the Subject Offenses.

Figure 1

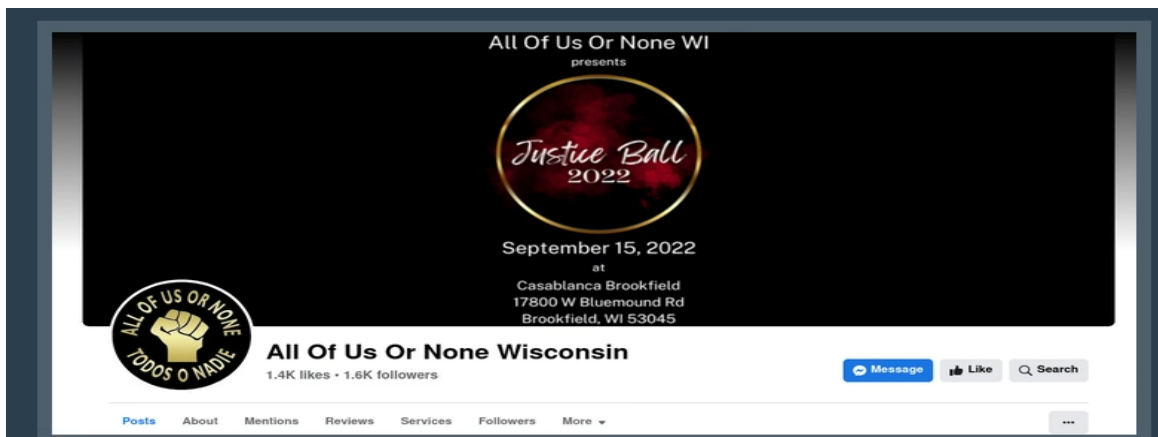


Figure 2



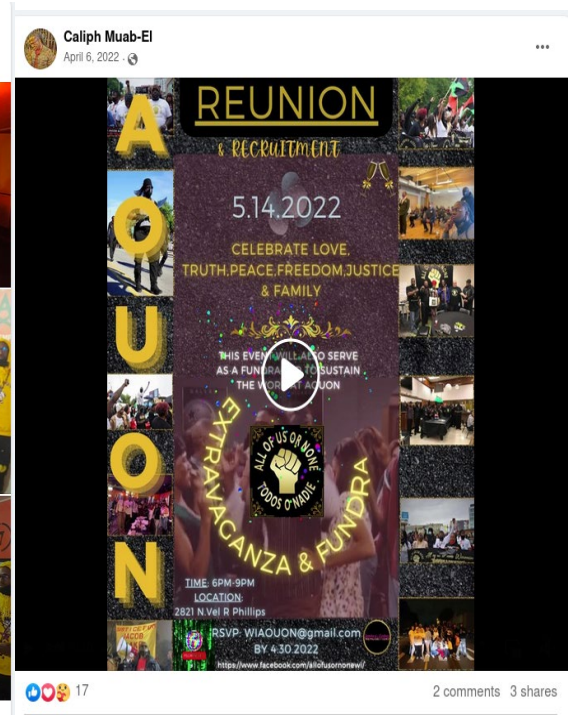
TARGET ACCOUNT 2

76. According to court ordered records, **Target Account 2** is subscribed to by MUAB-EL. The phone number verified to the account is subscribed to by MUAB-EL. Records indicate that MUAB-EL uses **Target Account 2** to exchange private messages to other subjects of the investigation including LAMON and the AGS from Florida. Below are screenshots (Figures 3 and 4) taken from MUAB-EL's publicly available Facebook posts from **Target Account 2**. Figure 3 references the BPSN gang, and Figure 4 references AOUON. Given the evidence discussed above vis-à-vis AOUON and the BPSN, MUAB-EL's connection to **Target Account 2**, and the private messages associated with **Target Account 2**, I believe this account is likely to contain communications or information pertaining to the Subject Offenses.

Figure 3



Figure 4



TARGET ACCOUNT 3

77. According to court ordered records, **Target Account 3** is subscribed to by Jason CLARKE. CHS #1 stated CLARKE was part of the “Ghost Crew,” which was the group of targets who traveled to Florida in October 2022 to harm an AGS, as described above in Paragraph 42. Figures 5 through 8 are screenshots taken from **Target Account 3**, including a post about the AGS (Figure 5). Given the evidence discussed above vis-à-vis the attack on the AGS, and the targets’ use of social media to advance their misconduct, I believe this account is likely to contain communications or information pertaining to the Subject Offenses.

Figure 5

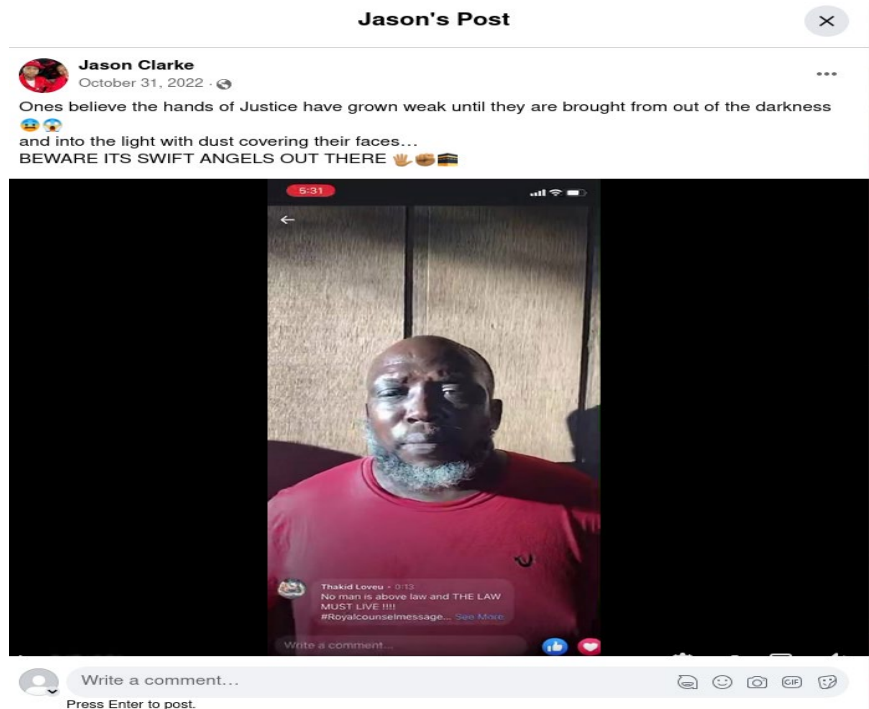


Figure 6



Figure 7



Figure 8



TARGET ACCOUNT 4

78. Open-source research revealed that LAMON and MUAB-EL are Facebook friends. On LAMON's publicly available Facebook page (**Target Account 4**), she represents herself as tax preparer for EMPIRE. Publicly available on LAMON's Facebook are the below screenshots: Figures 9, 10, and 11. The information listed on LAMON's Facebook posts corroborates information provided by CHS#1. Given the evidence discussed above vis-à-vis EMPIRE and LAMON and the public advertising regarding EMPIRE using **Target Account 4**, I believe this account is likely to contain communications or information pertaining to the subject offenses.

Figure 9



Figure 10

Ladrea Lamon
3d · 🌐

My problem is.....
it's not enough of y'all ready to file right now and come February 17th I'm try to have bout 5 figures on that check

Mannnnnn... they need to come on with y'all w2s...
matter fact y'all share this post I'm trying to let your self employed/1099 cousins come sign up since y'all gotta wait a few more days
If u can't stop thinking about your sister taxes then send her over here ima make sure she got enough to share 🤔🤔🤔

Free credit repair
Up to 9500 cash advance
Referral fees
Max refund allowable
Click the link to upload ur documents
Ladrea - <https://bit.ly/Taxclientform>





Figure 11



ladreal@etaxfirms.com TAX FIRM EMPIRE 414-949-0684

1 comment 2 shares

👍 Like 💬 Comment ➦ Share

Ladrea Lamon
Ladrea - <https://bit.ly/Taxclientform>

COGNITOFORMS.COM
Tax Client Intake Form | Cognito Forms

TARGET ACCOUNTS 5 & 6

79. An undercover agent (“UC”) with the IRS reached out to LAMON at number 414-949-0684 for the purpose of getting a tax return created. LAMON responded to the UC that her brother Robert Bishop would assist with the UC’s return. LAMON also posted the below screenshot (Figure 12) advertising for BISHOP on Facebook, using **Target Account 4**, on February 5, 2023.

80. BISHOP responded to the UC that he would assist in preparing a return for the UC. Below are screenshots (Figures 13, 14, and 15) from BISHOPS’ Facebook page (**Target Account 5**) which reflect his involvement in EMPIRE.

81. BISHOP also uses Instagram to post about EMPIRE. Figures 16 and 17 below are screenshots from BISHOP’s Instagram page (**Target Account 6**).

82. Given the evidence discussed above vis-à-vis EMPIRE and LAMON, the promised large refunds in BISHOP’s posts, and the advertising on these accounts, I believe these accounts are likely to contain communications or information pertaining to the Subject Offenses.

Figure 12



Figure 13

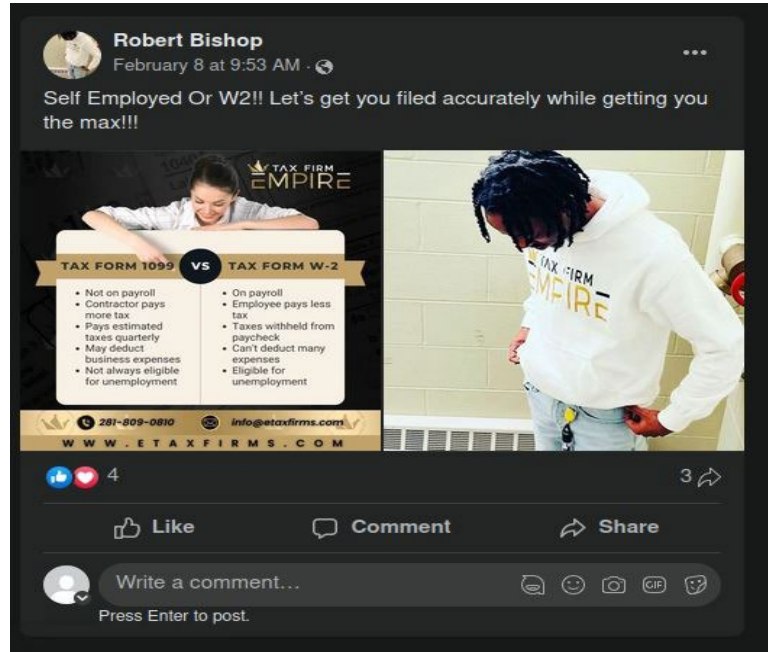


Figure 14



Figure 15

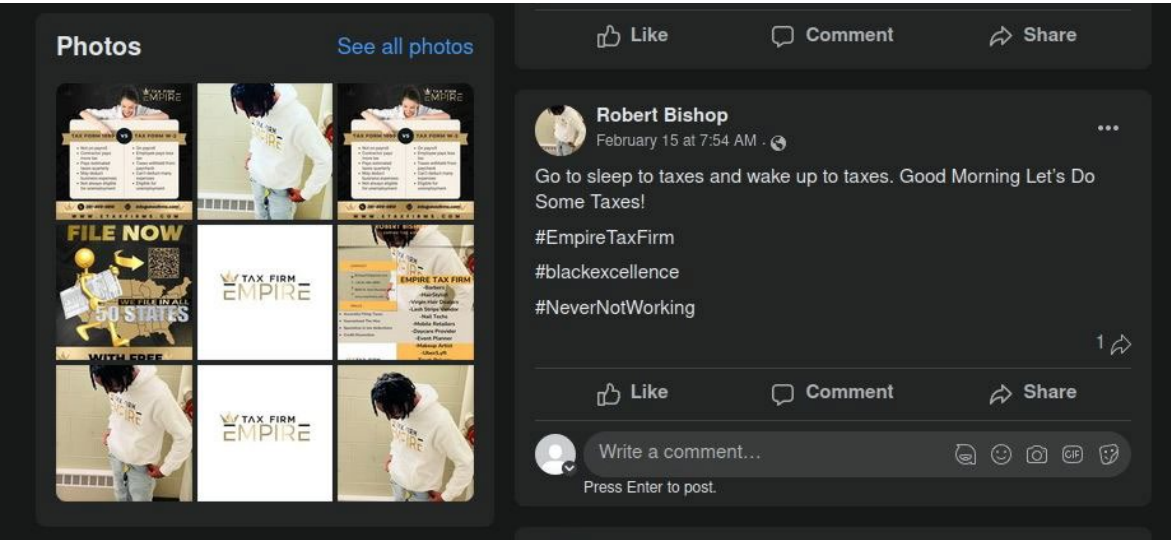


Figure 16

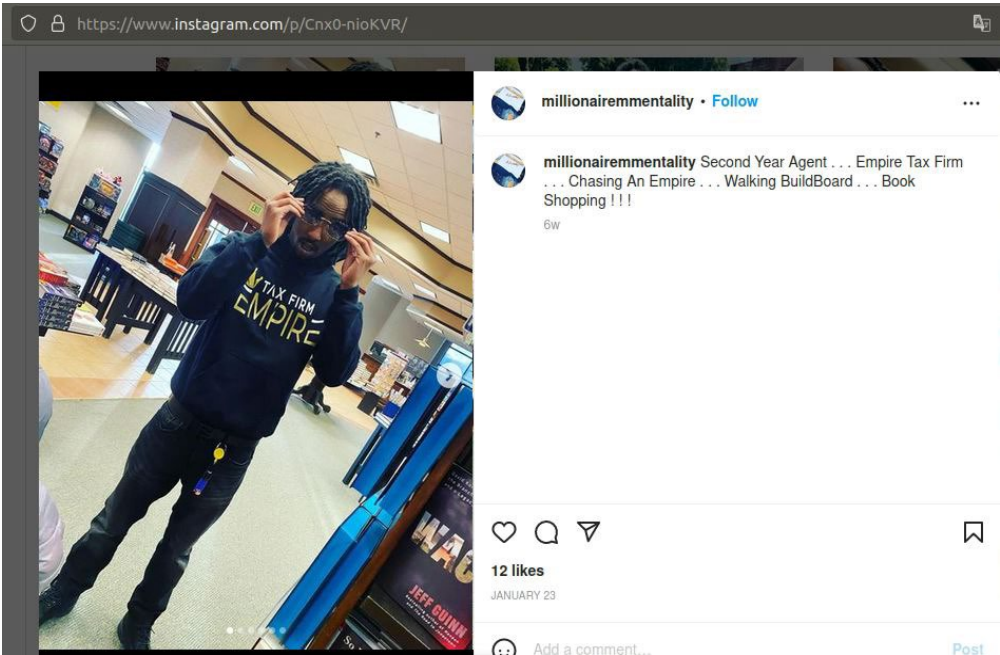
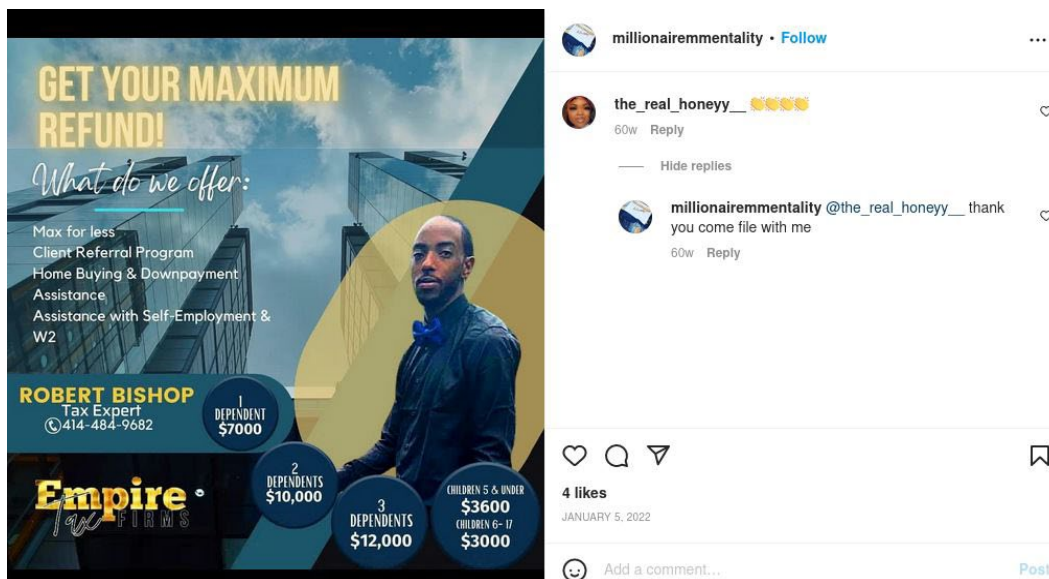


Figure 17



TARGET ACCOUNT 7

83. **Target Account 7** is MARTIN'S Facebook account. LW (a citizen witness regarding MARTIN, described above) provided law enforcement with screenshots and videos taken from this account. The videos provided are Facebook live videos wherein MARTIN discusses her tax business and the allegations being made that EMPIRE is committing fraud. Figure 18 was a screenshot provided by LW on or about February 22, 2023.

84. SS (another citizen witness regarding MARTIN, described above) provided similar material to law enforcement, also believed to be from **Target Account 7**. Figure 19 is a screenshot provided by SS on or about March 2, 2023, wherein MARTIN discusses mailing checks believed to be associated with EMPIRE.

85. Figure 20 below is another screenshot taken from **Target Account 7**, wherein MARTIN seemingly "offer[s] CASH" to individuals filing with EMPIRE.

Figure 18

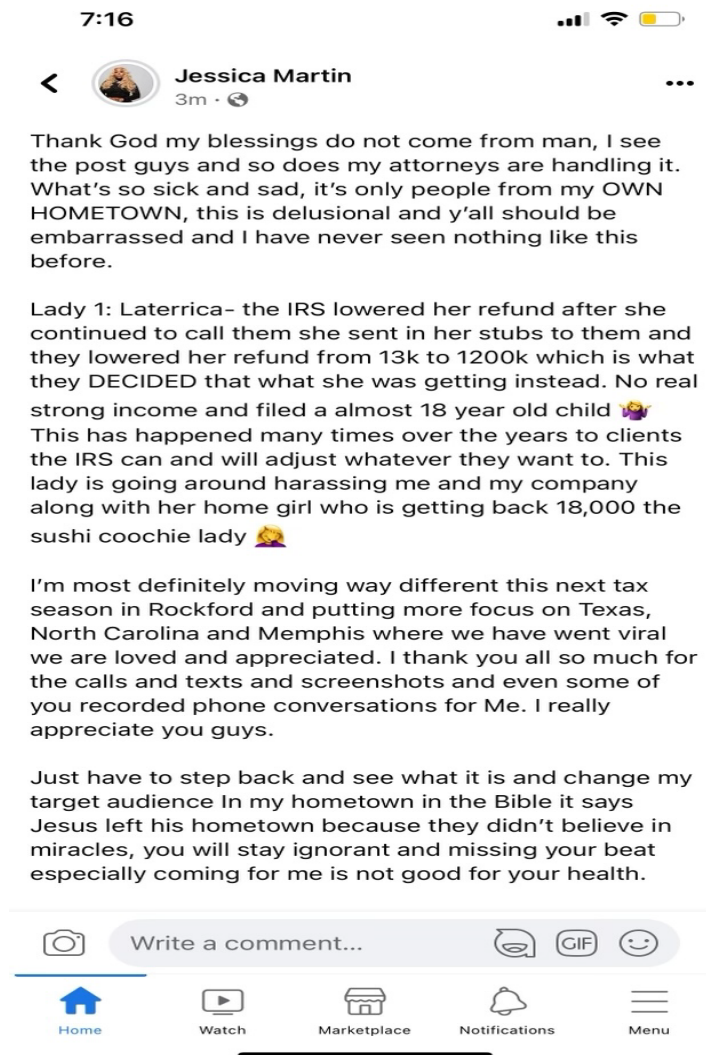


Figure 19

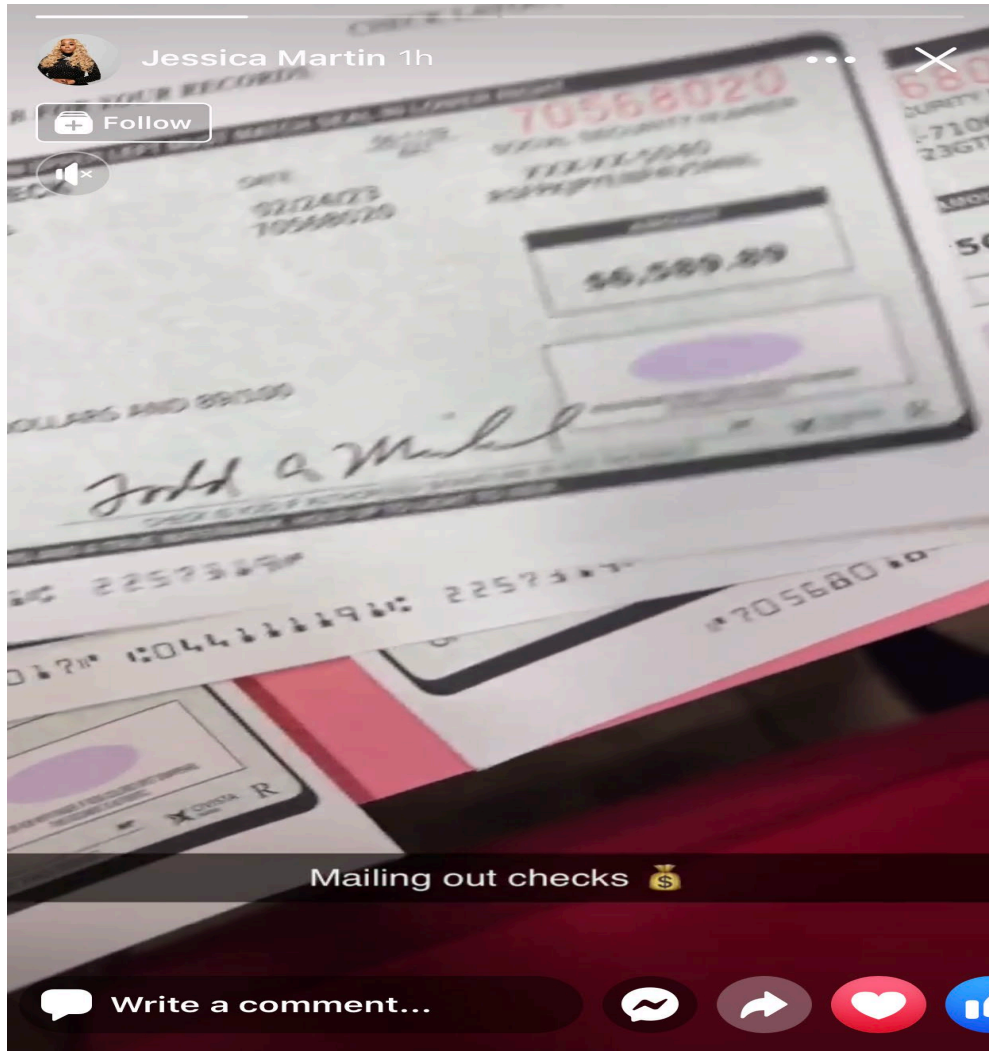


Figure 20



TARGET ACCOUNT 8

86. **Target Account 8** is another Facebook account maintained by MARTIN, wherein she posts regarding EMPIRE. Figures 21 and 22 below were taken **Target Account 8**. Given the evidence discussed above vis-à-vis MARTIN and her use of **Target Account 8** to promote EMPIRE, I believe this account is likely to contain communications or information pertaining to the subject offenses.

Figure 21

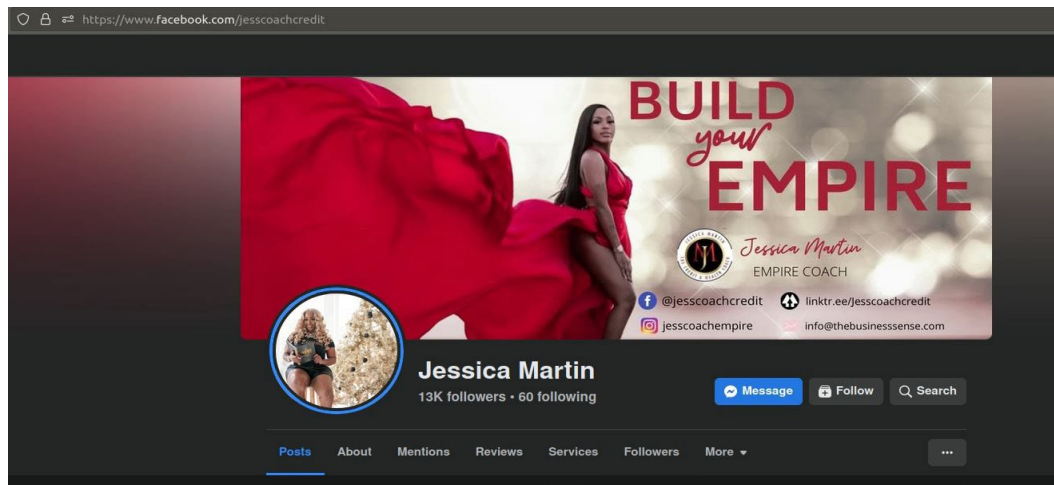
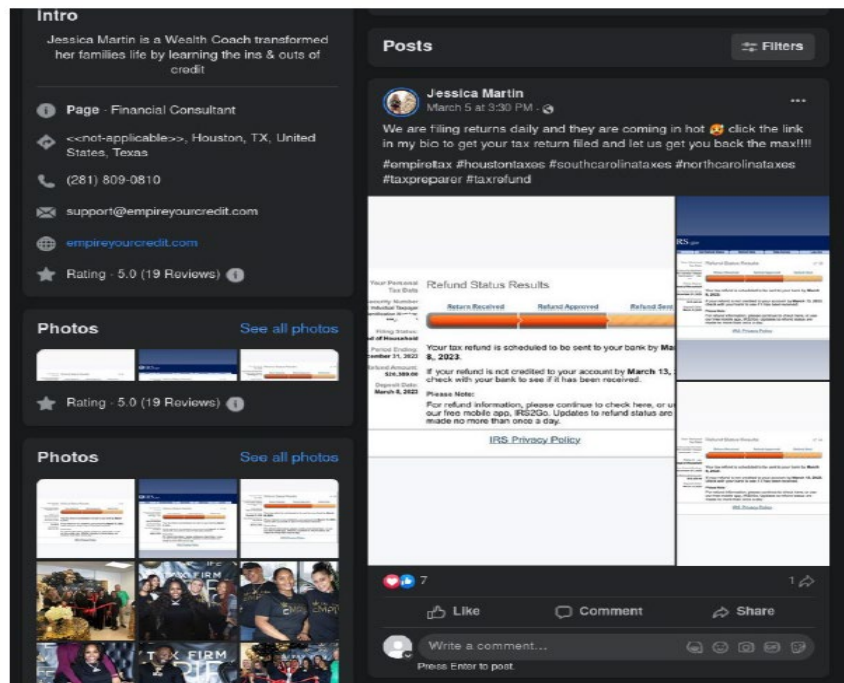


Figure 22



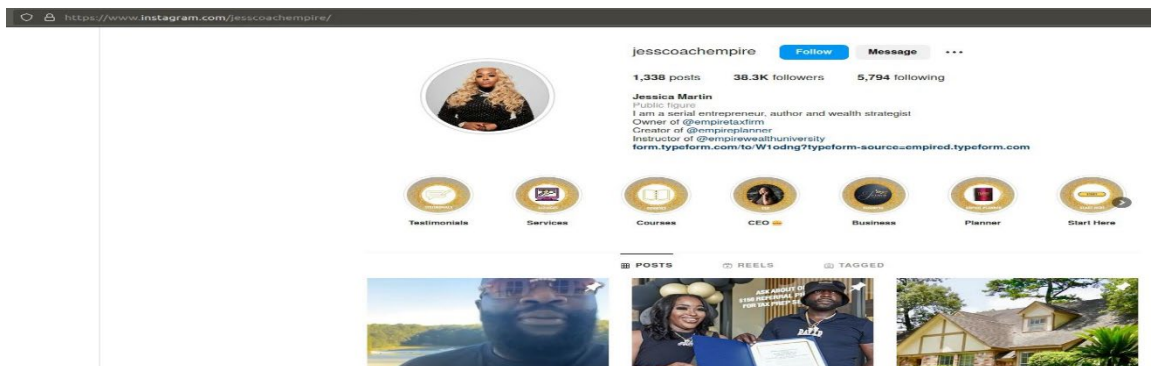
TARGET ACCOUNT 9

87. **Target Account 9** is an Instagram account maintained by MARTIN, wherein she posts regarding EMPIRE. Figures 23 and 24 below were taken **Target Account 9**. Given the evidence discussed above vis-à-vis MARTIN and her use of **Target Account 9** to promote EMPIRE, I believe this account is likely to contain communications or information pertaining to the subject offenses.

Figure 23



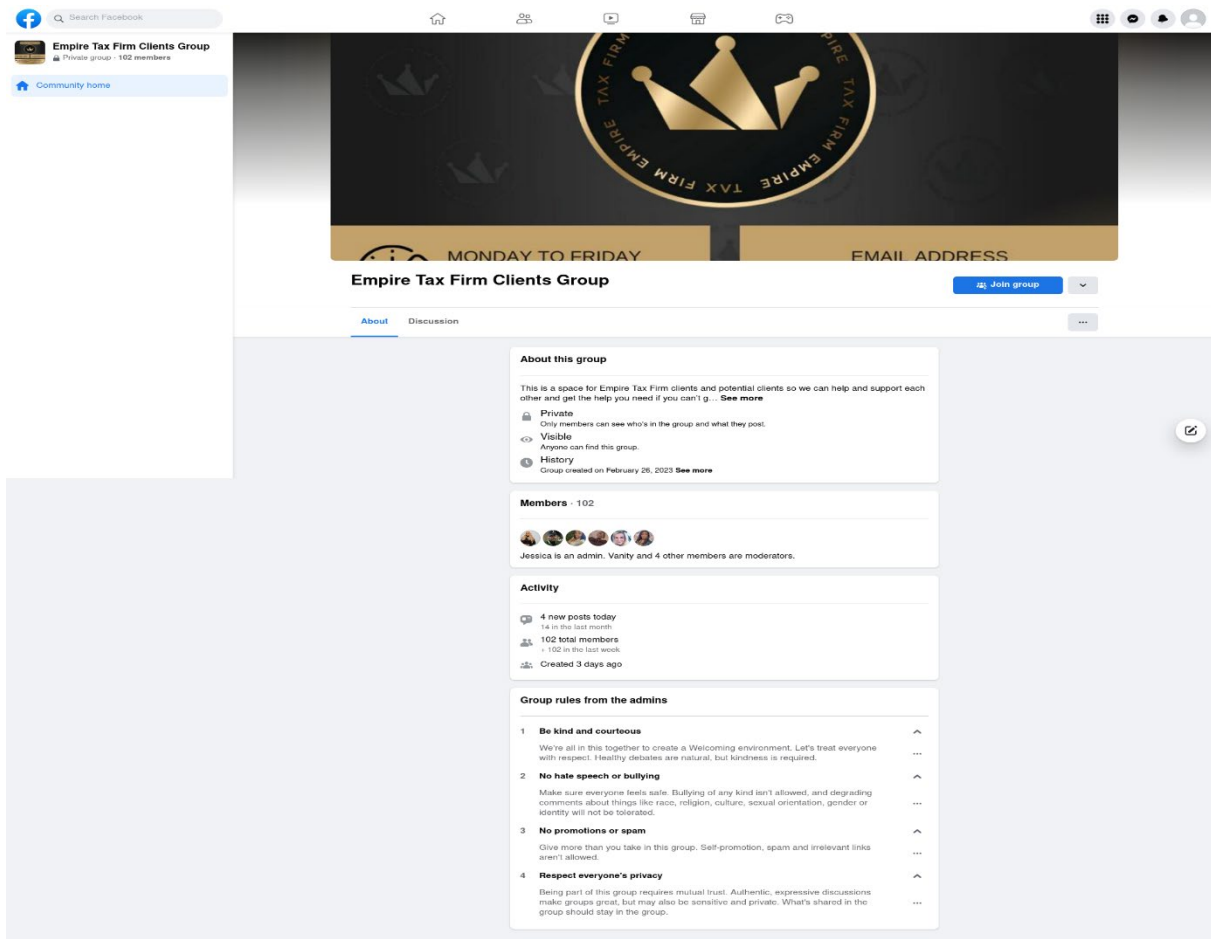
Figure 24



TARGET ACCOUNT 10

88. **Target Account 10** is a Facebook “group” moderated by MARTIN, wherein she posts regarding EMPIRE. Figure 25 below was taken from **Target Account 10**. Given the evidence discussed above vis-à-vis MARTIN, her use of **Target Account 10** to promote EMPIRE, and KC’s previously described information regarding EMPIRE’s conducting training over Facebook groups, I believe this account is likely to contain communications or information pertaining to the subject offenses.

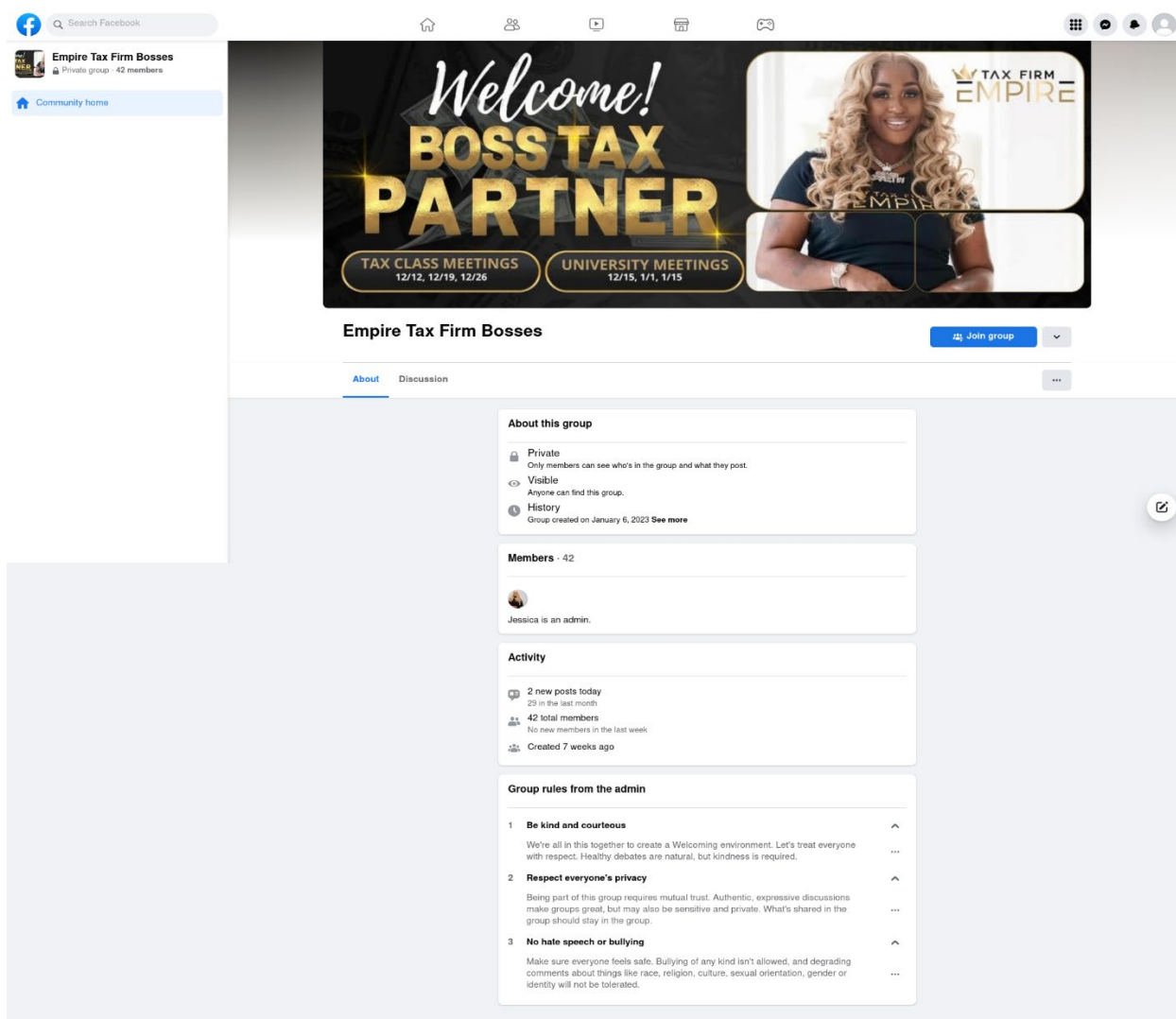
Figure 25



TARGET ACCOUNT 11

89. **Target Account 11** is another Facebook “group” moderated by MARTIN, wherein she posts regarding EMPIRE. Figure 26 below was taken from **Target Account 11**. Given the evidence discussed above vis-à-vis MARTIN, her use of **Target Account 11** to promote EMPIRE, and KC’s previously described information regarding EMPIRE’s conducting training over Facebook groups, I believe this account is likely to contain communications or information pertaining to the Subject Offenses.

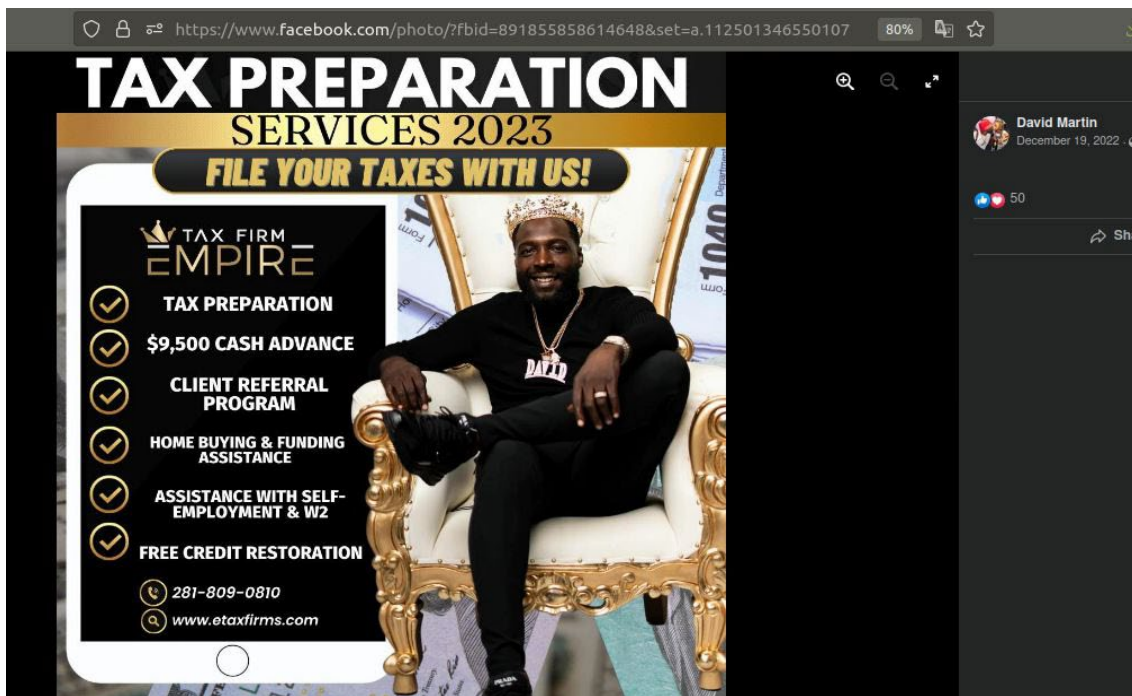
Figure 26



TARGET ACCOUNT 12

90. **Target Account 12** is a Facebook account maintained by DAVID, MARTIN's husband. As previously described, DAVID is a co-owner of EMPIRE with MARTIN. Figure 27 below (wherein DAVID promotes EMPIRE and offers a "\$9,500 cash advance" for customers) was taken from **Target Account 12**. Given the evidence discussed above vis-à-vis MARTIN, her relationship with DAVID, and DAVID's use of **Target Account 12** to promote EMPIRE, I believe this account is likely to contain communications or information pertaining to the Subject Offenses.

Figure 27



TARGET ACCOUNT 13

91. **Target Account 13** is an Instagram account maintained by DAVID, MARTIN's husband. As previously described, DAVID is a co-owner of EMPIRE with MARTIN. Figure 28 below (wherein DAVID once again promotes EMPIRE and offers a "\$9,500 cash advance" for customers) was taken from **Target Account 13**. Given the evidence

discussed above vis-à-vis MARTIN, her relationship with DAVID, and DAVID's use of **Target Account 13** to promote EMPIRE, I believe this account is likely to contain communications or information pertaining to the Subject Offenses.

Figure 28



TARGET ACCOUNT 14

92. **Target Account 14** is a Facebook page maintained in the name of EMPIRE itself. Figure 29 below (wherein EMPIRE tells customers to “add your family member to your company payroll and deduct their salaries”) was taken from **Target Account 14**. Given the evidence discussed above vis-à-vis EMPIRE and the seemingly unlawful exhortation reflected in Figure 29, I believe this account is likely to contain communications or information pertaining to the Subject Offenses.

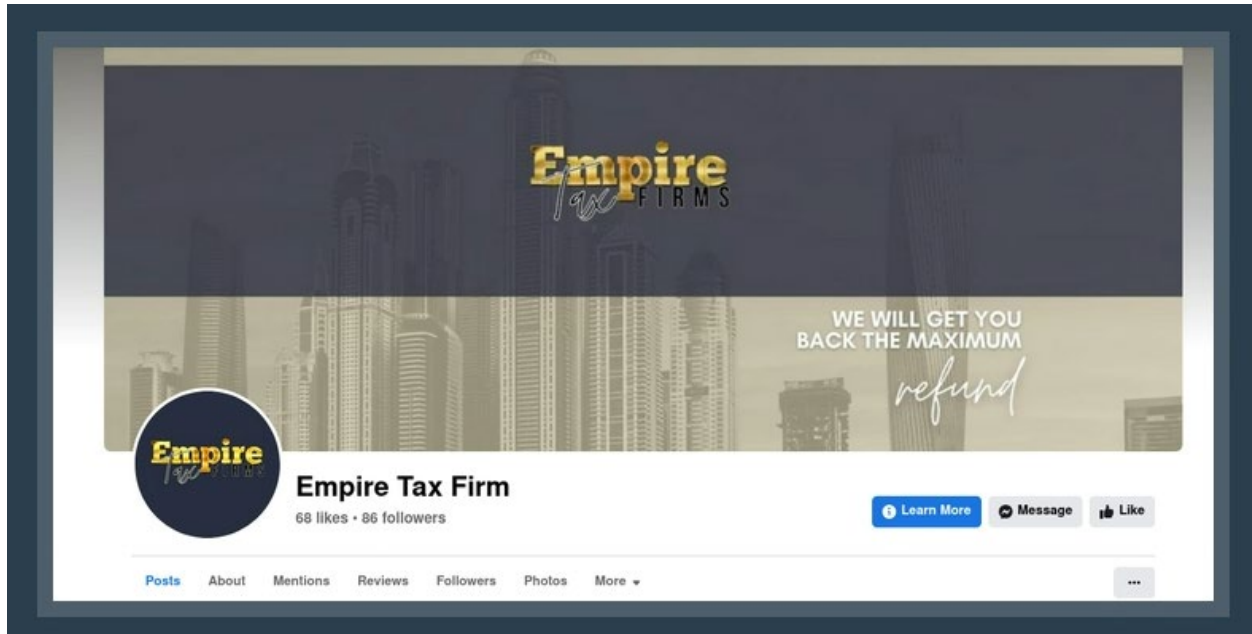


TARGET ACCOUNT 15

93. **Target Account 15** is another Facebook page maintained in the name of EMPIRE itself. Figure 30 below was taken from **Target Account 15**. Given the evidence discussed above vis-à-vis EMPIRE, EMPIRE's facial connection to **Target Account 15**, and EMPIRE's established pattern of using Facebook accounts in connection with the Subject

Offenses, I believe this account is likely to contain communications or information pertaining to the Subject Offenses.

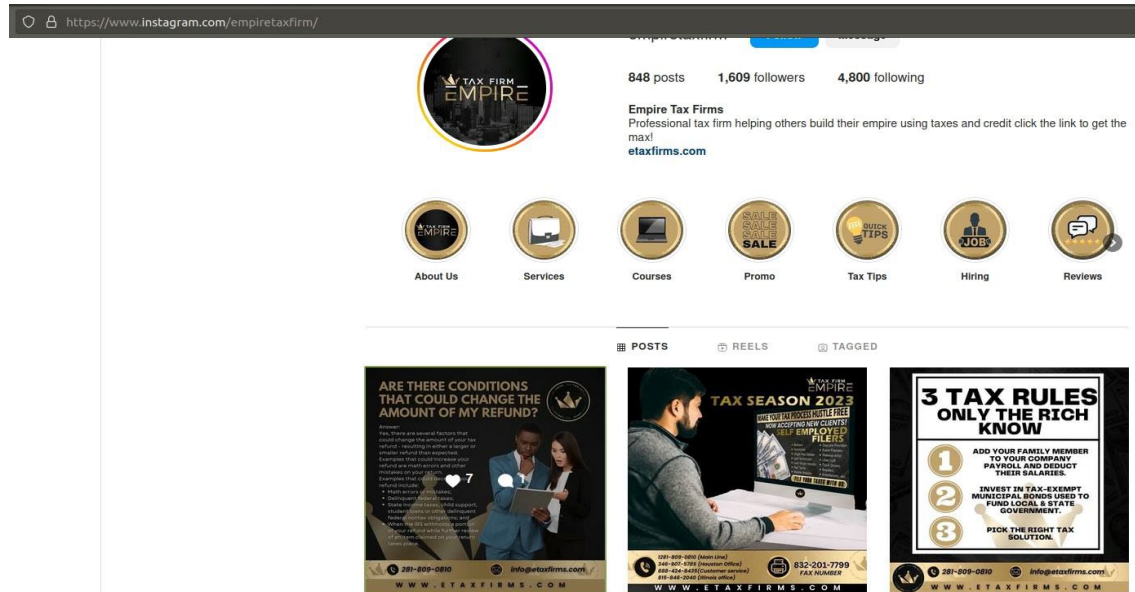
Figure 30



TARGET ACCOUNT 16

94. **Target Account 16** is an Instagram page maintained in the name of EMPIRE itself. Figure 31 below (wherein EMPIRE again tells customers to “add your family member to your company payroll and deduct their salaries”) was taken from **Target Account 16**. Given the evidence discussed above vis-à-vis EMPIRE, EMPIRE’s facial connection to **Target Account 16**, EMPIRE’s established pattern of using social media accounts in connection with the Subject Offenses, and the seemingly unlawful exhortation reflected in Figure 31, I believe this account is likely to contain communications or information pertaining to the Subject Offenses.

Figure 31



TARGET ACCOUNT 17

95. On or about March 24, 2023, LW contacted the FBI and provided that a Facebook group called Fraud by Empire Tax Firm Group (**Target Account 17**) was created for victims to discuss the fraud committed by EMPIRE and Martin. LW provided Figure 32, taken from **Target Account 17** to law enforcement. Figures 33 and 34 ARE screenshots taken by law enforcement of **Target Account 17** on or about April 5, 2023. There appear to be 62 members of the group who likely had a fraudulent tax return created by EMPIRE. Given the evidence discussed above vis-à-vis EMPIRE and the nature of the group depicted in Figures 32-34, I believe this account is likely to contain communications or information pertaining to the Subject Offenses.

Figure 32

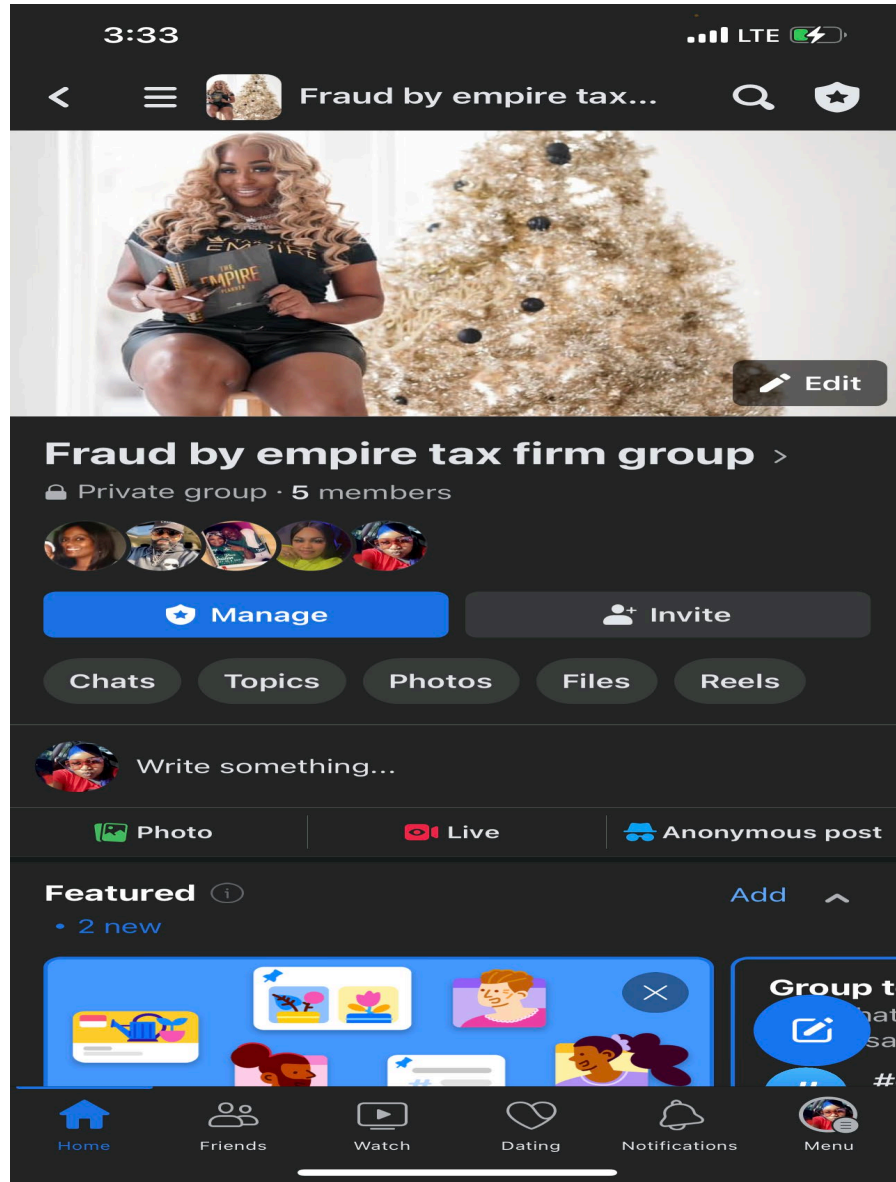


Figure 33

Fraud by empire tax firm group

Join group

AboutDiscussion

About this group

Have u been a victim of fraud by empire tax firm then this is the group for u
#jessicamartinempiretaxfirm #empiretaxfirm

Private

Only members can see who's in the group and what they post.




Visible

Anyone can find this group.

History

Group created on March 24, 2023 [See more](#)


Members · 62




Christina and 2 other members are admins.


Figure 34

Activity

 **3 new posts today**
73 in the last month



62 total members
No new members in the last week



Created a week ago

BACKGROUND CONCERNING FACEBOOK¹

96. Meta owns and operates Facebook, a free-access social networking website that can be accessed at <http://www.facebook.com>. Facebook users can use their accounts to share communications, news, photographs, videos, and other information with other Facebook users, and sometimes with the public.

97. Meta asks Facebook users to provide basic contact and personal identifying information either during the registration process or thereafter. This information may include the user's full name, birth date, gender, e-mail addresses, physical address (including city, state, and zip code), telephone numbers, screen names, websites, and other personal identifiers. Each Facebook user is assigned a user identification number and can choose a username.

98. Facebook users may join one or more groups or networks to connect and interact with other users who are members of the same group or network. Facebook assigns a group identification number to each group. A Facebook user can also connect directly with individual Facebook users by sending each user a "Friend Request." If the recipient of a "Friend Request" accepts the request, then the two users will become "Friends" for purposes of Facebook and can exchange communications or view information about each other. Each Facebook user's account includes a list of that user's "Friends" and a "News Feed," which

¹ The information in this section is based on information published by Meta on its Facebook website, including, but not limited to, the following webpages: "Privacy Policy," available at <https://www.facebook.com/privacy/policy>; "Terms of Service," available at <https://www.facebook.com/legal/terms>; "Help Center," available at <https://www.facebook.com/help>; and "Information for Law Enforcement Authorities," available at <https://www.facebook.com/safety/groups/law/guidelines/>.

highlights information about the user's "Friends," such as profile changes, upcoming events, and birthdays.

99. Facebook users can select different levels of privacy for the communications and information associated with their Facebook accounts. By adjusting these privacy settings, a Facebook user can make information available only to himself or herself, to Facebook users, or to anyone with access to the Internet, including people who are not Facebook users. A Facebook user can also create "lists" of Facebook friends to facilitate the application of these privacy settings. Facebook accounts also include other account settings that users can adjust to control, for example, the types of notifications they receive from Facebook.

100. Facebook users can create profiles that include photographs, lists of personal interests, and other information. Facebook users can also post "status" updates about their whereabouts and actions, as well as links to videos, photographs, articles, and other items available elsewhere on the Internet. Facebook users can also post information about upcoming "events," such as social occasions, by listing the event's time, location, host, and guest list. In addition, Facebook users can "check in" to locations or add their geographic locations to their Facebook posts, thereby revealing their geographic locations at particular dates and times. A particular user's profile page also includes a "Wall," which is a space where the user and his or her "Friends" can post messages, attachments, and links that will typically be visible to anyone who can view the user's profile.

101. Facebook users can upload photos and videos to be posted on their Wall, included in chats, or for other purposes. Users can "tag" other users in a photo or video and can be tagged by others. When a user is tagged in a photo or video, he or she generally receives a notification of the tag and a link to see the photo or video.

102. Facebook users can use Facebook Messenger to communicate with other users via text, voice, video. Meta retains instant messages and certain other shared Messenger content unless deleted by the user, and retains transactional records related to voice and video chats. Facebook users can also post comments on the Facebook profiles of other users or on their own profiles; such comments are typically associated with a specific posting or item on the profile.

103. If a Facebook user does not want to interact with another user on Facebook, the first user can “block” the second user from seeing his or her account.

104. Facebook has a “like” feature that allows users to give positive feedback or connect to pages. Facebook users can “like” Facebook posts or updates, as well as webpages or content on third-party (*i.e.*, non-Facebook) websites. Facebook users can also become “fans” of Facebook pages.

105. Facebook has a search function that enables its users to search Facebook for keywords, usernames, or pages, among other things.

106. Each Facebook account has an activity log, which is a list of the user’s posts and other Facebook activities from the inception of the account to the present. The activity log includes stories and photos that the user has been tagged in, as well as connections made through the account, such as “liking” a Facebook page or adding someone as a friend. The activity log is visible to the user but cannot be viewed by people who visit the user’s Facebook page.

107. Facebook also has a Marketplace feature, which allows users to post free classified ads. Users can post items for sale, housing, jobs, and other items on the Marketplace.

108. In addition to the applications described above, Meta provides users with access to thousands of other applications (“apps”) on the Facebook platform. When a Facebook user accesses or uses one of these applications, an update about that the user’s access or use of that application may appear on the user’s profile page.

109. Meta also retains records of which IP addresses were used by an account to log into or out of Facebook, as well as IP address used to take certain actions on the platform. For example, when a user uploads a photo, the user’s IP address is retained by Meta along with a timestamp.

110. Meta retains location information associated with Facebook users under some circumstances, such as if a user enables “Location History,” “checks-in” to an event, or tags a post with a location.

111. Social networking providers like Meta typically retain additional information about their users’ accounts, such as information about the length of service (including start date), the types of service utilized, and the means and source of any payments associated with the service (including any credit card or bank account number). In some cases, Facebook users may communicate directly with Meta about issues relating to their accounts, such as technical problems, billing inquiries, or complaints from other users. Social networking providers like Meta typically retain records about such communications, including records of contacts between the user and the provider’s support services, as well as records of any actions taken by the provider or user as a result of the communications.

112. As explained herein, information stored in connection with a Facebook account may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each

element or alternatively, to exclude the innocent from further suspicion. In my training and experience, a Facebook user's IP log, stored electronic communications, and other data retained by Meta, can indicate who has used or controlled the Facebook account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, profile contact information, private messaging logs, status updates, and tagged photos (and the data associated with the foregoing, such as date and time) may be evidence of who used or controlled the Facebook account at a relevant time. Further, Facebook account activity can show how and when the account was accessed or used. For example, as described herein, Meta logs the Internet Protocol (IP) addresses from which users access their accounts along with the time and date. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the account access and use relating to the crime under investigation. Such information allows investigators to understand the geographic and chronological context of Facebook access, use, and events relating to the crime under investigation. Additionally, location information retained by Meta may tend to either inculcate or exculpate the Facebook account owner. Last, Facebook account activity may provide relevant insight into the Facebook account owner's state of mind as it relates to the offense under investigation. For example, information on the Facebook account may indicate the owner's motive and intent to commit a crime (e.g., information indicating a plan to commit a crime), or consciousness of guilt (e.g., deleting account information to conceal evidence from law enforcement).

113. Therefore, the servers of Meta are likely to contain all the material described above, including stored electronic communications and information concerning subscribers

and their use of Facebook, such as account access information, transaction information, and other account information.

BACKGROUND CONCERNING INSTAGRAM²

114. Instagram is a service owned by Meta, a United States company and a provider of an electronic communications service as defined by 18 U.S.C. §§ 3127(1) and 2510. Specifically, Instagram is a free-access social networking service, accessible through its website and its mobile application, that allows subscribers to acquire and use Instagram accounts, like the target account(s) listed in Attachment A, through which users can share messages, multimedia, and other information with other Instagram users and the public.

115. Meta collects basic contact and personal identifying information from users during the Instagram registration process. This information, which can later be changed by the user, may include the user's full name, birth date, gender, contact e-mail addresses, physical address (including city, state, and zip code), telephone numbers, credit card or bank account number, and other personal identifiers. Meta keeps records of changes made to this information.

116. Meta also collects and retains information about how each user accesses and uses Instagram. This includes information about the Internet Protocol ("IP") addresses used to create and use an account, unique identifiers and other information about devices and web browsers used to access an account, and session times and durations.

² The information in this section is based on information published by Meta on its Instagram website, including, but not limited to, the following webpages: "Privacy Policy," <https://privacycenter.instagram.com/policy/>; "Information for Law Enforcement," <https://help.instagram.com/494561080557017>; and "Help Center," <https://help.instagram.com>.

117. Each Instagram account is identified by a unique username chosen by the user. Users can change their usernames whenever they choose but no two users can have the same usernames at the same time. Instagram users can create multiple accounts and, if “added” to the primary account, can switch between the associated accounts on a device without having to repeatedly log-in and log-out.

118. Instagram users can also connect their Instagram and Facebook accounts to utilize certain cross-platform features, and multiple Instagram accounts can be connected to a single Facebook account. Instagram accounts can also be connected to certain third-party websites and mobile apps for similar functionality. For example, an Instagram user can “tweet” an image uploaded to Instagram to a connected Twitter account or post it to a connected Facebook account or transfer an image from Instagram to a connected image printing service. Meta maintains records of changed Instagram usernames, associated Instagram accounts, and previous and current connections with accounts on Meta and third-party websites and mobile apps.

119. Instagram users can “follow” other users to receive updates about their posts and to gain access that might otherwise be restricted by privacy settings (for example, users can choose whether their posts are visible to anyone or only to their followers). Users can also “block” other users from viewing their posts and searching for their account, “mute” users to avoid seeing their posts, and “restrict” users to hide certain activity and prescreen their comments. Instagram also allows users to create a “close friends list” for targeting certain communications and activities to a subset of followers.

120. Users have several ways to search for friends and associates to follow on Instagram, such as by allowing Meta to access the contact lists on their devices to identify

which contacts are Instagram users. Meta retains this contact data unless deleted by the user and periodically syncs with the user's devices to capture changes and additions. Users can similarly allow Meta to search an associated Facebook account for friends who are also Instagram users. Users can also manually search for friends or associates.

121. Each Instagram user has a profile page where certain content they create and share ("posts") can be viewed either by the public or only the user's followers, depending on privacy settings. Users can customize their profile by adding their name, a photo, a short biography ("Bio"), and a website address.

122. One of Instagram's primary features is the ability to create, edit, share, and interact with photos and short videos. Users can upload photos or videos taken with or stored on their devices, to which they can apply filters and other visual effects, add a caption, enter the usernames of other users ("tag"), or add a location. These appear as posts on the user's profile. Users can remove posts from their profiles by deleting or archiving them. Archived posts can be reposted because, unlike deleted posts, they remain on Meta's servers.

123. Users can interact with posts by liking them, adding or replying to comments, or sharing them within or outside of Instagram. Users receive notification when they are tagged in a post by its creator or mentioned in a comment (users can "mention" others by adding their username to a comment followed by "@"). An Instagram post created by one user may appear on the profiles or feeds of other users depending on a number of factors, including privacy settings and which users were tagged or mentioned.

124. An Instagram "story" is similar to a post but can be viewed by other users for only 24 hours. Stories are automatically saved to the creator's "Stories Archive" and remain

on Meta's servers unless manually deleted. The usernames of those who viewed a story are visible to the story's creator until 48 hours after the story was posted.

125. Instagram allows users to broadcast live video from their profiles. Viewers can like and add comments to the video while it is live, but the video and any user interactions are removed from Instagram upon completion unless the creator chooses to send the video to IGTV, Instagram's long-form video app.

126. Instagram Direct, Instagram's messaging service, allows users to send private messages to select individuals or groups. These messages may include text, photos, videos, posts, videos, profiles, and other information. Participants to a group conversation can name the group and send invitations to others to join. Instagram users can send individual or group messages with "disappearing" photos or videos that can only be viewed by recipients once or twice, depending on settings. Senders can't view their disappearing messages after they are sent but do have access to each message's status, which indicates whether it was delivered, opened, or replayed, and if the recipient took a screenshot. Instagram Direct also enables users to video chat with each other directly or in groups.

127. Instagram offers services such as Instagram Checkout and Facebook Pay for users to make purchases, donate money, and conduct other financial transactions within the Instagram platform as well as on Facebook and other associated websites and apps. Instagram collects and retains payment information, billing records, and transactional and other information when these services are utilized.

128. Instagram has a search function which allows users to search for accounts by username, user activity by location, and user activity by hashtag. Hashtags, which are topical words or phrases preceded by a hash sign (#), can be added to posts to make them more easily

searchable and can be “followed” to generate related updates from Instagram. Meta retains records of a user’s search history and followed hashtags.

129. Meta collects and retains location information relating to the use of an Instagram account, including user-entered location tags and location information used by Meta to personalize and target advertisements.

130. Meta uses information it gathers from its platforms and other sources about the demographics, interests, actions, and connections of its users to select and personalize ads, offers, and other sponsored content. Meta maintains related records for Instagram users, including information about their perceived ad topic preferences, interactions with ads, and advertising identifiers. This data can provide insights into a user’s identity and activities, and it can also reveal potential sources of additional evidence.

131. In some cases, Instagram users may communicate directly with Meta about issues relating to their accounts, such as technical problems, billing inquiries, or complaints from other users. Social networking providers like Meta typically retain records about such communications, including records of contacts between the user and the provider’s support services, as well as records of any actions taken by the provider or user as a result of the communications.

132. For each Instagram user, Meta collects and retains the content and other records described above, sometimes even after it is changed by the user (including usernames, phone numbers, email addresses, full names, privacy settings, email addresses, and profile bios and links).

133. In my training and experience, evidence of who was using Instagram and from where, and evidence related to criminal activity of the kind described above, may be found in

the files and records described above. This evidence may establish the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or, alternatively, to exclude the innocent from further suspicion.

134. For example, the stored communications and files connected to an Instagram account may provide direct evidence of the offenses under investigation. Based on my training and experience, [[instant messages, voice messages, photos, videos, and documents]] are often created and used in furtherance of criminal activity, including to communicate and facilitate the offenses under investigation.

135. Determining identity and locating the targets of the investigations will be important in determining who is involved in the tax scheme or BPSN activity. In addition, the user’s account activity, logs, stored electronic communications, and other data retained by Meta can indicate who has used or controlled the account. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. For example, subscriber information, [[messaging logs, photos, and videos (and the data associated with the foregoing, such as date and time)]] may be evidence of who used or controlled the account at a relevant time. As an example, because every device has unique hardware and software identifiers, and because every device that connects to the Internet must use an IP address, IP address and device identifier information can help to identify which computers or other devices were used to access the account. Such information also allows investigators to understand the geographic and chronological context of access, use, and events relating to the crime under investigation.

136. Account activity may also provide relevant insight into the account owner's state of mind as it relates to the offenses under investigation. For example, information on the account may indicate the owner's motive and intent to commit a crime (e.g., information indicating a plan to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

137. Other information connected to the use of Instagram may lead to the discovery of additional evidence. For example, associated and linked accounts, stored communications, photos, and videos may reveal services used in furtherance of the crimes under investigation or services used to communicate with co-conspirators. In addition, stored communications, contact lists, photos, and videos can lead to the identification of co-conspirators and instrumentalities of the crimes under investigation.

138. Therefore, Meta's servers are likely to contain stored electronic communications and information concerning subscribers and their use of Instagram. In my training and experience, such information may constitute evidence of the crimes under investigation including information that can be used to identify the account's user or users.

INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

139. I anticipate executing this warrant under the Electronic Communications Privacy Act, 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require Meta to disclose to the government copies of the records and other information (including the content of communications) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

CONCLUSION

140. Based on the foregoing, I request that the Court issue the proposed search warrant.

141. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant. The government will execute this warrant by serving it on Meta. Because the warrant will be served on Meta, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

ATTACHMENT A

Matter No. 2022R00210

Property to Be Searched

This warrant applies to information associated with following social media accounts (the “Target Accounts”), for which the associated data is stored at premises owned, maintained, controlled, or operated by Meta Platforms, Inc., headquartered in Menlo Park, California:

- a. Facebook Account: UID: 103183581120331 (**Target Account 1**)
- b. Facebook Account: UID: 100004443158401 (**Target Account 2**)
- c. Facebook Account: UID: 100063503829690 (**Target Account 3**)
- d. Facebook Account: UID: 1003158861 (**Target Account 4**)
- e. Facebook.com/bighomie.rob; UID: 100037412529073 (**Target Account 5**)
- f. Instagram.com/millionairementality; UID: 210030646 (**Target Account 6**)
- g. Facebook Account: UID: 100013113481774 (**Target Account 7**)
- h. Facebook Account: UID: 100063752476178 (**Target Account 8**)
- i. Instagram Account: UID: 1296285044 (**Target Account 9**)
- j. Facebook Account(Group): 229347966182445. URL:
facebook.com/groups/229347966182445 (**Target Account 10**)
- k. Facebook Account(Group): 545401084294236. URL:
facebook.com/groups/545401084294236 (**Target Account 11**)
- l. Facebook Account::; UID: 100033707269327 (**Target Account 12**)
- m. Instagram.com/mr_david_martin UID: 341470073 (**Target Account 13**)
- n. Facebook Account: UID: 100063561696774 (**Target Account 14**)
- o. Facebook Account: UID: 100063862190767 (**Target Account 15**)
- p. Instagram Account: UID: 26331965215 (**Target Account 16**)

q. Facebook Account (Group) UID 242867438180983, URL:

<https://www.facebook.com/groups/242867438180983> (**Target Account 17**)

ATTACHMENT B

Matter No. 2022R00210

Particular Things to be Seized

I. Information to be disclosed by Meta Platforms, Inc. (“Meta”)

To the extent that the information described in Attachment A is within the possession, custody, or control of Meta, regardless of whether such information is located within or outside of the United States, including any messages, records, files, logs, or information that have been deleted but are still available to Meta, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Meta is required to disclose the following information to the government for each user ID listed in Attachment A:

- (a) All contact and personal identifying information, including full name, user identification number, birth date, gender, contact e-mail addresses, physical address (including city, state, and zip code), telephone numbers, screen names, websites, and other personal identifiers.
- (b) All activity logs for the account and all other documents showing the user’s posts and other Facebook activities from January 1, 2020 to the present.
- (c) All photos and videos uploaded by that user ID and all photos and videos uploaded by any user that have that user tagged in them from January 1, 2020 to the present including Exchangeable Image File (“EXIF”) data and any other metadata associated with those photos and videos;
- (d) All profile information; News Feed information; status updates; videos, photographs, articles, and other items; Notes; Wall postings; friend lists, including the friends’ Facebook user identification numbers; groups and networks of which

- the user is a member, including the groups' Facebook group identification numbers; future and past event postings; rejected "Friend" requests; comments; gifts; pokes; tags; and information about the user's access and use of Facebook applications;
- (e) All records or other information regarding the devices and internet browsers associated with, or used in connection with, that user ID, including the hardware model, operating system version, unique device identifiers, mobile network information, advertising ID, and user agent string;
 - (f) All other records and contents of communications and messages made or received by the user from January 1, 2020 to the present including all Messenger activity, private messages, chat history, video and voice calling history, and pending "Friend" requests;
 - (g) All "check ins" and other location information;
 - (h) All IP logs, including all records of the IP addresses that logged into the account;
 - (i) All records of the account's usage of the "Like" feature, including all Facebook posts and all non-Facebook webpages and content that the user has "liked";
 - (j) All information about the Facebook pages that the account is or was a "fan" of;
 - (k) All past and present lists of friends created by the account;
 - (l) All records of Facebook searches performed by the account from January 1, 2020 to the present.
 - (m) All information about the user's access and use of Facebook Marketplace;
 - (n) The types of service utilized by the user;

- (o) The length of service (including start date) and the means and source of any payments associated with the service (including any credit card or bank account number);
- (p) All privacy settings and other account settings, including privacy settings for individual Facebook posts and activities, and all records showing which Facebook users have been blocked by the account;
- (q) Records of any Facebook accounts that are linked to the account by machine cookies (meaning all Facebook user IDs that logged into Facebook by the same machine as the account); and
- (r) All records pertaining to communications between Meta and any person regarding the user or the user's Facebook account, including contacts with support services and records of actions taken.

Meta is hereby ordered to disclose the above information to the government within 30 days of issuance of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, evidence and instrumentalities of violations of 18 U.S.C. § 371 (conspiracy to violate the laws of the United States); 18 U.S.C. § 1343 (wire fraud); 21 U.S.C. § 841 (unlawful possession and distribution of controlled substances); and 26 U.S.C. § 7206 (false statement in connection with tax submission) (the "Subject Offenses") since January 1, 2020, including, for each user ID identified on Attachment A, information pertaining to the following matters:

- (a) Evidence pertaining to gang activity to include, sale of illegal drugs, acts of violence, and fraudulent business activity.

- (b) The creation, preparation, and filing of tax returns, including all preparatory steps and communications.
- (c) Information provided by clients and potential clients concerning potential tax returns and PPP loans.
- (d) Records and information pertaining to taxes, refunds, and W-2s.
- (e) Advertisements and/or solicitation of tax clients.
- (f) Stimulus checks and Paycheck Protection Program Applications
- (g) Personal identifiable information of taxpayers, including names, date of birth, social security numbers, and driver's licenses.
- (h) 8. Proceeds and/or payments pertaining to the Subject Offenses.
- (i) 9. Financial records, including account information, bank statements, checks, money orders, cash, ATMs, withdrawals, deposits, transfers (including wire, ACH transfers);
- (j) All evidence of who created, used, owned or controlled the Target Accounts,
- (k) including, records that help reveal the identity and whereabouts of such person(s).
- (l) 11. Evidence indicating how and when the Target Account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crimes under investigation and to the Target Account owner.
- (m) Evidence indicating the Target Account(s) owner's state of mind as it relates to the crime under investigation.
- (n) The identity of the person(s) who communicated with the Target Accounts about matters relating to the above-mentioned violations, including records that hel reveal their whereabouts.

This warrant authorizes a review of electronically stored information, communications, other records and information disclosed pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

May 15, 2023

s/ D. Olszewski

Deputy Clerk, U.S. District Court
Eastern District of Wisconsin

UNITED STATES DISTRICT COURT

for the

Eastern District of Wisconsin

In the Matter of the Search of)

(Briefly describe the property to be searched
or identify the person by name and address))Records and information associated with 17)
social media accounts (See Attachments))

Case No. 23 MJ 91

Matter No.: 2022R00210

WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search and seizure of the following person or property located in the _____ District of _____

(identify the person or describe the property to be searched and give its location):

See Attachment A.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal (identify the person or describe the property to be seized):

See Attachment B.

YOU ARE COMMANDED to execute this warrant on or before 5/29/2023 (not to exceed 14 days)

☐ in the daytime 6:00 a.m. to 10:00 p.m. ☒ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to _____

Hon. William E. Duffin
(United States Magistrate Judge)☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized (check the appropriate box)☐ for _____ days (not to exceed 30) ☐ until, the facts justifying, the later specific date of _____

Date and time issued: 5/15/2023 at 11:03 AM

William E. Duffin

Judge's signature

City and state: Milwaukee, WI

Hon. William E. Duffin, U.S. Magistrate Judge

Printed name and title

Return

Case No.:

Date and time warrant executed:

Copy of warrant and inventory left with:

Inventory made in the presence of :

Inventory of the property taken and name(s) of any person(s) seized:

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

Executing officer's signature

Printed name and title

ATTACHMENT A

Matter No. 2022R00210

Property to Be Searched

This warrant applies to information associated with following social media accounts (the “Target Accounts”), for which the associated data is stored at premises owned, maintained, controlled, or operated by Meta Platforms, Inc., headquartered in Menlo Park, California:

- a. Facebook Account: UID: 103183581120331 (**Target Account 1**)
- b. Facebook Account: UID: 100004443158401 (**Target Account 2**)
- c. Facebook Account: UID: 100063503829690 (**Target Account 3**)
- d. Facebook Account: UID: 1003158861 (**Target Account 4**)
- e. Facebook.com/bighomie.rob; UID: 100037412529073 (**Target Account 5**)
- f. Instagram.com/millionairementality; UID: 210030646 (**Target Account 6**)
- g. Facebook Account: UID: 100013113481774 (**Target Account 7**)
- h. Facebook Account: UID: 100063752476178 (**Target Account 8**)
- i. Instagram Account: UID: 1296285044 (**Target Account 9**)
- j. Facebook Account(Group): 229347966182445. URL:
facebook.com/groups/229347966182445 (**Target Account 10**)
- k. Facebook Account(Group): 545401084294236. URL:
facebook.com/groups/545401084294236 (**Target Account 11**)
- l. Facebook Account::; UID: 100033707269327 (**Target Account 12**)
- m. Instagram.com/mr_david_martin UID: 341470073 (**Target Account 13**)
- n. Facebook Account: UID: 100063561696774 (**Target Account 14**)
- o. Facebook Account: UID: 100063862190767 (**Target Account 15**)
- p. Instagram Account: UID: 26331965215 (**Target Account 16**)

q. Facebook Account (Group) UID 242867438180983, URL:

<https://www.facebook.com/groups/242867438180983> (**Target Account 17**)

ATTACHMENT B

Matter No. 2022R00210

Particular Things to be Seized

I. Information to be disclosed by Meta Platforms, Inc. (“Meta”)

To the extent that the information described in Attachment A is within the possession, custody, or control of Meta, regardless of whether such information is located within or outside of the United States, including any messages, records, files, logs, or information that have been deleted but are still available to Meta, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Meta is required to disclose the following information to the government for each user ID listed in Attachment A:

- (a) All contact and personal identifying information, including full name, user identification number, birth date, gender, contact e-mail addresses, physical address (including city, state, and zip code), telephone numbers, screen names, websites, and other personal identifiers.
- (b) All activity logs for the account and all other documents showing the user’s posts and other Facebook activities from January 1, 2020 to the present.
- (c) All photos and videos uploaded by that user ID and all photos and videos uploaded by any user that have that user tagged in them from January 1, 2020 to the present including Exchangeable Image File (“EXIF”) data and any other metadata associated with those photos and videos;
- (d) All profile information; News Feed information; status updates; videos, photographs, articles, and other items; Notes; Wall postings; friend lists, including the friends’ Facebook user identification numbers; groups and networks of which

- the user is a member, including the groups' Facebook group identification numbers; future and past event postings; rejected "Friend" requests; comments; gifts; pokes; tags; and information about the user's access and use of Facebook applications;
- (e) All records or other information regarding the devices and internet browsers associated with, or used in connection with, that user ID, including the hardware model, operating system version, unique device identifiers, mobile network information, advertising ID, and user agent string;
 - (f) All other records and contents of communications and messages made or received by the user from January 1, 2020 to the present including all Messenger activity, private messages, chat history, video and voice calling history, and pending "Friend" requests;
 - (g) All "check ins" and other location information;
 - (h) All IP logs, including all records of the IP addresses that logged into the account;
 - (i) All records of the account's usage of the "Like" feature, including all Facebook posts and all non-Facebook webpages and content that the user has "liked";
 - (j) All information about the Facebook pages that the account is or was a "fan" of;
 - (k) All past and present lists of friends created by the account;
 - (l) All records of Facebook searches performed by the account from January 1, 2020 to the present.
 - (m) All information about the user's access and use of Facebook Marketplace;
 - (n) The types of service utilized by the user;

- (o) The length of service (including start date) and the means and source of any payments associated with the service (including any credit card or bank account number);
- (p) All privacy settings and other account settings, including privacy settings for individual Facebook posts and activities, and all records showing which Facebook users have been blocked by the account;
- (q) Records of any Facebook accounts that are linked to the account by machine cookies (meaning all Facebook user IDs that logged into Facebook by the same machine as the account); and
- (r) All records pertaining to communications between Meta and any person regarding the user or the user's Facebook account, including contacts with support services and records of actions taken.

Meta is hereby ordered to disclose the above information to the government within 30 days of issuance of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, evidence and instrumentalities of violations of 18 U.S.C. § 371 (conspiracy to violate the laws of the United States); 18 U.S.C. § 1343 (wire fraud); 21 U.S.C. § 841 (unlawful possession and distribution of controlled substances); and 26 U.S.C. § 7206 (false statement in connection with tax submission) (the "Subject Offenses") since January 1, 2020, including, for each user ID identified on Attachment A, information pertaining to the following matters:

- (a) Evidence pertaining to gang activity to include, sale of illegal drugs, acts of violence, and fraudulent business activity.

- (b) The creation, preparation, and filing of tax returns, including all preparatory steps and communications.
- (c) Information provided by clients and potential clients concerning potential tax returns and PPP loans.
- (d) Records and information pertaining to taxes, refunds, and W-2s.
- (e) Advertisements and/or solicitation of tax clients.
- (f) Stimulus checks and Paycheck Protection Program Applications
- (g) Personal identifiable information of taxpayers, including names, date of birth, social security numbers, and driver's licenses.
- (h) 8. Proceeds and/or payments pertaining to the Subject Offenses.
- (i) 9. Financial records, including account information, bank statements, checks, money orders, cash, ATMs, withdrawals, deposits, transfers (including wire, ACH transfers);
- (j) All evidence of who created, used, owned or controlled the Target Accounts,
- (k) including, records that help reveal the identity and whereabouts of such person(s).
- (l) 11. Evidence indicating how and when the Target Account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crimes under investigation and to the Target Account owner.
- (m) Evidence indicating the Target Account(s) owner's state of mind as it relates to the crime under investigation.
- (n) The identity of the person(s) who communicated with the Target Accounts about matters relating to the above-mentioned violations, including records that hel reveal their whereabouts.

This warrant authorizes a review of electronically stored information, communications, other records and information disclosed pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.